NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2008-06 Cyber Security Order 706
Draft CIP-002-4 Informal Review

The Cyber Security Order 706 Standard Drafting Team thanks all commenters who submitted comments on the proposed CIP-002-4 changes. These standards were posted for a 30-day informal comment period from May 4, 2010 through June 3, 2010. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 119 sets of comments. The complete record of comments submitted is posted on the Project 2008-06 Version 4 CIP Standards page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards, Herb Schrayshuen at (404) 446-2560 or at Herb.Schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

Index to Questions, Comments, and Responses

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Larry Bugh	ReliabilityFirst Staff										
2.	Group	Ruth Blevins	Dominion Resources Services, Inc.										
3.	Group	Guy Zito	Northeast Power Coordinating Council										
4.	Group	Kenneth D. Brown	Public Service Enterprise Group companies										
5.	Group	Sasa Maljukan	Hydro One										
6.	Group	David Grubbs	Garland Power and Light										
7.	Group	Roger Powers	CWLP Electric Transmission, Distribution and Operations Department										
8.	Group	Guy Andrews	GTC & GSOC										
9.	Group	Tommy Drea - CIP Compliance	Dairyland Power Cooperative										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
10.	Group	Joseph DePoorter	Madison Gas and Electric Company										
11.	Group	Carol Gerou	MRO's NERC Standards Review Subcommittee										
12.	Group	Denise Koehn	Bonneville Power Administration										
13.	Group	Steve Alexanderson	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group										
14.	Group	Richard Kafka	Pepco Holdings, Inc. - Affiliates										
15.	Group	Mark Stefaniak	Detroit Edison										
16.	Group	Frank Gaffney	Florida Municipal Power Agency										
17.	Group	Nathan Mitchell	APPA Task Force										
18.	Group	Sheryl Byrd	GE Energy										
19.	Group	Ben Li	IRC Standards Review Committee										
20.	Group	John Van Boxtel	WECC										
21.	Individual	Brent Ingebrigtson	E.ON U.S.										
22.	Individual	Ronald J Slack	Exelon Corporation										
23.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)										
24.	Individual	John Lawrence	Reliability & Compliance Group										
25.	Individual	Rick Terrill	Luminant										
26.	Individual	Linda Jacobson	FEUS										
27.	Individual	Robert Ulmer	American Transmission Company										
28.	Individual	John Brockhan	CenterPoint Energy										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
29.	Individual	Susan Kurtain	Regulatory Compliance										
30.	Individual	Paul Reymann, CEO	ReymannGroup, Inc.										
31.	Individual	Silvia Parada Mitchell	NextEra Energy Corporate Compliance										
32.	Individual	Boyd Nation	Southern Company										
33.	Individual	Tracey Stewart	Southwestern Power Administration										
34.	Individual	Donald Brookhyser	Cogeneration Association of California and Energy Producers & Users Coalition										
35.	Individual	David Batz	EEI										
36.	Individual	Tom Bradish	RRI Energy										
37.	Individual	Dora Moreno	Southern California Edison Company										
38.	Individual	Sandra Shaffer	PacifiCorp										
39.	Individual	Jana Van Ness	Arizona Public Service Company										
40.	Individual	Casey Hashimoto	Turlock Irrigation District										
41.	Individual	Ken Stratton	US Army Corps of Engineers, Omaha District										
42.	Individual	Michael Gammon	Kansas City Power & Light										
43.	Individual	John Alberts	Wolverine Power										
44.	Individual	Mike Hendrix	Idaho Power Company										
45.	Individual	Tony Dodge	BCTC										
46.	Individual	Greg Froehling	Green Country Energy										
47.	Individual	Roger Fradenburgh	Network & Security Technologies Inc										
48.	Individual	John Alberts	Wolverine Power										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
49.	Individual	John Kutzer	Consultant										
50.	Individual	Melissa Kurtz	USACE - Omaha Anchor										
51.	Individual	James Stanton	SPS Consulting Group Inc.										
52.	Individual	Michael Puscas	Northeast Utilities System										
53.	Individual	Roger Pan	Emerson Process Management										
54.	Individual	Jo Ann Newton	PNM Resources, Inc.										
55.	Individual	John Hughes	Electricity Consumers Resource Council (ELCON)										
56.	Individual	Ted Risher	Ingleside Cogeneration, LP										
57.	Individual	Thad Ness	American Electric Power										
58.	Individual	Ed Goff	Progress Energy (non-Nuclear)										
59.	Individual	Mark Thompson	Alberta Electric System Operator										
60.	Individual	Dan Roethemeyer	Dynegy Inc.										
61.	Individual	CJ Ingersoll	Constellation Energy Control and Dispatch, LLC										
62.	Individual	Daniel Duff	Liberty Electric Power, LLC										
63.	Individual	Jonathan Appelbaum	The United Illuminating Co										
64.	Individual	Greg Hataway	Powersouth Energy Cooperative										
65.	Individual	Kasia Mihalchuk	Manitoba Hydro										
66.	Individual	Steven Belle	SCE&G										
67.	Individual	William Gross	Nuclear Energy Institute										
68.	Individual	Randy Schimka	San Diego Gas and Electric Co.										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
69.	Individual	Brandy A. Dunn	Western Area Power Administration										
70.	Individual	Eric Scott	Ameren										
71.	Individual	Jim Simpson	Allegheny Energy Supply										
72.	Individual	Neal Williams	Poplar Bluff Municipal Utilities										
73.	Individual	E Hahn	MWDSC										
74.	Individual	Ed Nagy	LCEC										
75.	Individual	Paul Crosby	Platte River Power Authority										
76.	Individual	Showin Fu	US Army Corps of Engineers										
77.	Individual	SPP RE Staff	Southwest Power Pool Regional Entity										
78.	Individual	William F. Watson	Old Dominion Electric Cooperative										
79.	Individual	Michael R. Lombardi	Northeast Utilities										
80.	Individual	Shawn Barrett	Michigan Public Power Agency										
81.	Individual	Fred Meyer	The Empire District Electric Company										
82.	Individual	Darryl Curtis	Oncor Electric Delivery LLC										
83.	Individual	Andres Lopez	USACE HQ										
84.	Individual	Peter Yost	Con Edison of New York										
85.	Individual	Bill Keagle	BGE										
86.	Individual	Michael Albosta	SRW Cogeneration Limited Partnership										
87.	Individual	Martin Bauer	US Bureau of Reclamation										
88.	Individual	Bob Mathews	Pacific Gas & Electric Company										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
89.	Individual	Barbara Kedrowski	We Energies										
90.	Individual	Saurabh Saksena	National Grid										
91.	Individual	Sungly Chiu	LADWP										
92.	Individual	Kenneth A. Goldsmith	Alliant Energy										
93.	Individual	Amir Y. Hammad	Constellation Power Source Generation										
94.	Individual	Kevin Cyr	Seattle City Light										
95.	Individual	Steve Newman	MidAmerican Energy Company										
96.	Individual	Bob Case	Black Hills Corporation										
97.	Individual	Jason Marshall	Midwest ISO										
98.	Individual	Steve Toth	Covanta Energy										
99.	Individual	Jon Kapitz	Xcel Energy										
100.	Individual	William J. Smith	Allegheny Power										
101.	Individual	Donovan Tindill	Matrikon Inc.										
102.	Individual	Patrick Stava	Nebraska Public Power District										
103.	Individual	Greg Rowland	Duke Energy										
104.	Individual	Kathleen Goodman	ISO New England Inc										
105.	Individual	David Martorana	Tenaska										
106.	Individual	Doug Hohlbaugh	FirstEnergy Corporation										
107.	Individual	John Falsey	Edison Mission Marketing and Trading										
108.	Individual	Stephen C. Knapp	Constellation Energy Commodities Group Inc.										

		Commenter	Organization	Industry Segment									
				1	2	3	4	5	6	7	8	9	10
109.	Individual	Eric Ruskamp	Lincoln Electric System										
110.	Individual	Randi Woodward	Minnesota Power										
111.	Individual	Kevin Koloini	American Municipal Power										
112.	Individual	Dave Norton	Entergy										
113.	Individual	Christine Hasha	ERCOT ISO										
114.	Individual	John Allen	City Utilities of Springfield, Missouri										
115.	Individual	Rex A Roehl	Indeck Energy Services, Inc										
116.	Individual	Cynthia Broadwell	Progress Energy - Nuclear Generation										
117.	Individual	Dan Rochester	Independent Electricity System Operator										
118.	Individual	Catherine Koch	Puget Sound Energy										
119.	Individual	Ernie Hayden	Verizon Business										

1. **Do you agree with the adoption of the following new or revised terms and their definitions for inclusion in the NERC Glossary: BES Cyber System Component, BES Cyber System, and Control Center? If not, please explain and supply your proposed modification.**

   1.a. **BES Cyber System Component — One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.**

Summary Consideration:

Many commenters expressed concerns about the inclusion of software and data within the definition of BES Cyber System Component. One commenter observed that the definition should only include devices with routable connectivity. Many observed the laundry list of functions should be removed and replaced with the function that is more specific to the operation of the BES. A number of commenters proposed alternative language for the definition.

The SDT considered these comments and decided to define the term BES Cyber Asset to focus on the "real-time" impact on the "Reliability Operating Services" of the BES, which include those functions performed for the reliable operation of the BES. This definition now provides the foundation for the definition of BES Cyber Systems. In addition, the SDT has included clarification in the definition on the 15-minute characterization of "real-time."

The new proposed definition of **BES Cyber System** is: *One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.*

The new proposed definition of **BES Cyber Asset** is: *A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset.*

The SDT has also modified the definition of Cyber Asset to make it more specific to the device and remove ambiguity on the exact nature of what is included in the definition of the Cyber Asset.

#	Organization	Yes or No	Question 1.a. Comment
1.a	WECC		Although this language is directly from the Federal Power Act, describing electronic devices as “hardware, software and data” is redundant and inaccurate. Electronic software and data reside on some type of hardware in all cases. Suggest removing the parenthetical as it is confusing and data is addressed later in the definition and the definition is clearer without it.If data is to be addressed in the standard it should be defined and addressed separately. The word “organized” is imprecise in this context; “Implemented,” “deployed,” or “utilized” may be a better word.The following rewrite is one proposed alternative.BES Cyber System Component - A programmable electronic device utilized in a BES Cyber System.
2.a	BGE	Agree with proposed definition	1.a and 1.b should be reversed. Disposition should be defined.
3.a	Old Dominion Electric Cooperative	Agree with proposed definition	Agreement is under the assumption that the present NERC definition of BES (e.g. =>100 kV) stands.
4.a	Progress Energy - Nuclear Generation	Agree with proposed definition	Define Disturbance
5.a	Florida Municipal Power Agency	Agree with proposed definition	FMPA agrees with the intent of the definition but believes that the definition can be improved significantly. FMPA offers the following simpler definition:”A programmable electronic device which responds to a BES condition or Disturbance, or enables control and operation of the BES.”For the following reasons: (i) “one or more” seems to

#	Organization	Yes or No	Question 1.a. Comment
			describe a system, not a singular component; (ii) we do not understand how “data” can be a component; and (iii) we do not understand the value of the “laundry list” of things components do and believe the focus should be on how the component impacts the BES.
6.a	Bonneville Power Administration	Agree with proposed definition	Greatly improved. Use of "...which respond..." clarifies that the standard is talking about control systems. However, please leave the parenthetical "(including hardware, software and data)" out. It is a bit confusing since data can't do any of the things listed. By definition a cyber system is made up of the hardware, the software and the data that allows it to operate. It appears that the punctuation in this definition is incorrect. We suggest:”One or more programmable electronic devices organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data which respond to a BES condition or Disturbance or enables control and operation.”
7.a	Dynegy Inc.	Agree with proposed definition	I agree but request additional detail examples be provided to determine specifically what these items are.
8.a	National Grid	Agree with proposed definition	National Grid agrees with the definition but seeks clarification from the SDT if the examples cited below will be considered as BES Cyber System Component:1) As part of the Burn Management System (BMS) in the power plant, the programmable PLC device is used along with the connected thermo-couples to monitor the temperature for fuel burning. If the temperature readings are wrong, the PLC can be programmed to take action to increase the fuel input or to limit/shutoff the fuel. This could have an immediate or short term effect (within 15 minutes). The amount of fuel determines what the output of the unit will be. Is the PLC or the entire BMS (including the PLC) BES Cyber Component? 2) Generating plant connects to Transmission Substation. There are programmable microprocessor relays installed within the substation for power plant / transmission line protection. Are these microprocessor relays BES Cyber Components?

#	Organization	Yes or No	Question 1.a. Comment
			3) The new BES Cyber System Component could also include the Exciter system that exists at Northport PS. Once again, could the PLC or the entire system, including the computer, be part of the BES Cyber Systems? 4) Another system that potentially could be included under the newer broad definition would be the Precipitator Rapper system. This system has a PLC that handles the Rappers. The system is not critical to Operations, however, under a broad definition that includes the 15-minute rule, if the Rappers failed, the unit(s) could be limited due to environmental compliance. The Precipitator Rappers are not connected to any network and are isolated.
9.a	Dairyland Power Cooperative	Agree with proposed definition	Shorten the name to BES Cyber Component.
10.a	Reliability & Compliance Group	Agree with proposed definition	The definition is O.K. Need to add BES to Disturbance and BES to enable control and operation. It would be more helpful if the definition “BES” were included in this document
11.a	Black Hills Corporation	Agree with proposed definition	The definition should include tie back to “BES Cyber System” as inserted above.
12.a	FEUS	Agree with proposed definition	The drafting team should consider clarifying; or enable or control and operation "of BES" or "greater than xxkV" This could be interpreted as an RTU in a 13.8kv sub serving only customer load.
13.a	PacifiCorp	Disagree with	: PacifiCorp agrees with EEI’s suggested alternative definition::BES Cyber System Component - One or more programmable electronic devices (including hardware)

#	Organization	Yes or No	Question 1.a. Comment
		proposed definition	organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: o Voice Communication systems o media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to the reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance the reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed. In addition, the definition of "programmable" should be provided. Is a device that is "set" considered to be programmable?
14.a	Allegheny Energy Supply	Disagree with proposed definition	1) Does this definition need to cover more than a single device since a BES Cyber System is a collection of these? 2) Software and data should not be included in this definition. Protection of the software and data should be included in security requirements but not in the definition itself. Additionally these are both terms that are easily interpreted in different ways.3) It is difficult to get a clear understanding of what the terms "disposition" and "maintenance" mean in this context.4) Suggest: BES Cyber System Component - A programmable electronic device (including hardware), that is part of a BES Cyber System, providing input/output, processing, information storage, communications, human interaction (display, trending, alarming / alerting, input, etc.),

#	Organization	Yes or No	Question 1.a. Comment
			or maintenance, which is necessary for a BES Cyber System to fully perform its function.
15.a	Consultant	Disagree with proposed definition	1. Inclusion of the word 'communication' would seem to imply that communication equipment is included in the definition. Should be clarified to clearly state what aspects of communication, if any, is included.2. A 'component' would seem to be inconsistent with 'organized for the...' A component performs an activity, the 'system' would consist of 'components organized for the...'3. Software and Data are not programmable devices. Device implies hardware; if software and data are to be included the component definition should be clarified. What is software in terms of the definition? Operating system, application, database, word processing, executable files, scripts, and batch files...4. Component is singular - programmable electronic devices is plural. This is inconsistent. Suggest identifying a component (hardware, software, or data) as singular terms.5. I think "data" should be removed from this definition. Suggested new definition: BES Cyber System Component: hardware or software that performs one of the following functions (1) input, (2) processing, (3) storage, or (4) output of data that enables control or operation of a BES Cyber System.5.BES condition has no meaning. It is not a defined term, and therefore is vague. Suggest removing this wording or clarifying the intent.6. "... enable control or operation." - Of what, and when. All the time or only during a Disturbance? Needs clarification of the intent of this phrase.7. devices... for... display of data..." It is unclear how a display device could be compromised resulting in a degradation of the BES? 8. There is published literature that addresses the concepts of Cyber-Physical Systems that distinguishes between 'hardware components', 'software components', and 'bridge components' as the makeup of cyber-physical systems. This would appear to be a better framework for defining components than the listing of multiple functions, which dims the "bright lines" for consistently defining and categorizing the many variations and configurations within the industry.
16.a	Progress Energy (non-Nuclear)	Disagree with proposed	1. We feel programmable electronic devices is too broad. Also, it seems that there should be a distinction between firmware versus a traditional OS.2. From a generation perspective, these would be likely be in scope and shouldn't be - foundation field bus, device Net, smart transmitters (Rosemount), RS232/485 Serial connections and

#	Organization	Yes or No	Question 1.a. Comment
		definition	electronic protection relaying. We need to know if this would include DCS “Smart” field instrumentation using non-routable network protocols such as Foundation Fieldbus, DeviceNet, Hart, etc. Just about every instrument connected to plant automation system is a programmable electronic device. Per CIP 11 definitions of routable and non-routable they would be considered non-routable. We need examples of components included and components that would not be included. Possibly include examples for generation facilities, ECC’s and transmission. This could include Generator Protection Panels, PLC’s, EX2000 Generator exciter, Bentley Nevada vibration system, Medium Voltage Switch gear protective relays, motor protection relays, etc, etc. These are all “Programmable” and can be accessed via non-routable, ISO layer 1&2 hardware programming by MODBUS. All these devices are already INSIDE the protected Electric and Physical perimeter umbrella.3. The Standards definitions still seem to still be written to traditional PC and IT Business platforms. The standards need to be written to target single use industrial control systems.4. Based on this definition a microprocessor relay associated with a transmission line would be in consideration as a cyber component. If a device has burned in programming, maybe it is considered but classified low impact. User programmable devices may be a higher impact. Many programmable devices may not support use banners. Redundancy will not allow us to remove devices from scope.5. This reads like an ‘or’ definition. In that case, communication connectivity is not required for a device to be considered as a cyber system component. That needs to be very clear since with past standards we were evaluating based on external connectivity and routable vs. non-routable protocols.6. What constitutes a BES "condition"? 7. If definition is limited to the "organized" Cyber subsystems (e.g. 1.b. below) we can work with that. Attachment II appears to define the impact per Cyber System not component level. Suggest removal of component level definition and focus on system level issues.8. Proprietary protocols should not be included.9.Need clarification on what ‘programmable’ means. Recommended definition: Capable of dynamically accepting a sequence of operations to be automatically performed (a device which includes only firmware defined logic which cannot be dynamically changed - such as an EPROM - would not be included). Consider clarification between

#	Organization	Yes or No	Question 1.a. Comment
			programmable and configurable.10. Strike “one or more” because “one or more” implies a system not a component
17.a	Platte River Power Authority	Disagree with proposed definition	A “System Component” should be singular. For example: BES Cyber System Component - A programmable electronic device (to include the hardware, software and data) used for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which responds to a BES condition or disturbance; or enables control and operation.
18.a	LCEC	Disagree with proposed definition	A BES Cyber System Component should not be described as "One or more". Systems can contain more than one component but components should not consist of more than one device. Enable control and operation needs to describe what is being controlled or operated.
19.a	USACE - Omaha Anchor	Disagree with proposed definition	A) This definition could include phone systems - which according to the committee were not meant to be included in this standard. Has any thought been given to an exclusion table or specifically excluding telephone systems? B) Has any thought been given to separating out classification by operating system (OS)? - Ex. Windows, Unix, Solaris - high OS; PLC - low OS or general computing device. We are still going to have TFE issues with a lot of the low OS components.
20.a	Nuclear Energy Institute	Disagree with proposed definition	Agree with the exception that: Question 2 indicates that the definition of BES Cyber System bounds the scope to real-time operations systems, yet it is not clear from the proposed definition of BES Cyber System Component. Consider revising to:”One or more programmable electronic devices (including hardware, software and data) organized for the real-time collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.”Lastly, the term “organize for” should be clarified by description such that a set of one-or-more programmable electronic devices constituting a BES Cyber System Component may be treated as a single system with respect to the application of requirements in CIP 011-1. This would preclude a debate

#	Organization	Yes or No	Question 1.a. Comment
			about how far down into an electronic device(s) the analysis must be performed. For example, a device with two programmable logic controllers on a single board may be treated as one BES Cyber System Component rather than individually as two BES Cyber System Components. Another example might include a turbine control system with vibration monitors. The collection of programmable electronic devices supporting the turbine control system including the monitors is a single BES Cyber System Component.
21.a	NextEra Energy Corporate Compliance	Disagree with proposed definition	At the workshop the drafting team requested that the industry point out comments that move the Version 4 forward, and any fatal flaws. The comments of NextEra Energy (and its affiliates, which include NextEra Resources and Florida Power & Light Company) (NextEra) will focus on constructive comments and fatal flaws. At this time, it appears that CIP-010 does not provide the proper foundation to build a CIP Standard that is well defined, so that the industry, the Regional Entities, NERC and FERC can all understand what is being protected, what is not being protected, or what should be protected via CIP-011. CIP-010 is thus fatally flawed. It is our opinion that CIP-010 should not offer the industry, auditors and regulators such flexibility to second guess each other, which is seen currently. Rather CIP-010 should have very clear definitions of what is the Control Center, what are the Transmission and Generation Cyber Systems that need to be protect and what are the BES Cyber System Components that must be protected for the identified Cyber Systems associated with Control Centers, Generators and Transmission. The flexibility protective options and performance based approach should be in CIP-011. Accordingly, NextEra requests that the drafting team develop a specific definition of what is and is not a BES Cyber System for Control Centers, for Generators, for Transmission - and list for each the BES Cyber Components that need to be protected in each. Given the short period of time from the workshop to these comments, NextEra was not able to propose definitions or lists, but NextEra will be working such and proposing them in the future. NextEra strongly recommends that the drafting team reconsider its flexibility approach in CIP-010 and requests, from the industry, specific definitions of what is and is not a BES Cyber System for Control Centers, for Generators, and for Transmission and a list for each of the BES Cyber Components that need to be protected in each. In this spirit, NextEra recommends the following edits.BES Cyber

#	Organization	Yes or No	Question 1.a. Comment
			System Component - A programmable electronic device (including hardware, software and data) listed below. At Control Centers, BES Cyber System Components are:(List)At Transmission Facilities, BES Cyber Systems Components are:(List)At Generation Facilities, BES Cyber Systems Components are:(List)
22.a	BCTC	Disagree with proposed definition	BCTC does not consider this a good definition as more clarity is required. The following are specific areas where BCTC feels the definition should be revised: - removal of the word “communication” “software” and “data” are not programmable devices. Their placement within the definition is confusing The definition is very “loose”. BCTC would like the definition to be more clear as to what is a cyber system component (i.e. must such a component have a routable protocol, etc.) - right now we find it difficult to grasp this concept based on the current definition When referring to BES System Components (and BES System) clarification is required as to whether we are referring to just ‘production’ environments; development or quality assurance environments are excluded from scope? If you have components of the BES Cyber System (i.e. EMS) which are considered LOW impact, can you segregate/ isolate these devices on a separate network segment w/ firewall so that these components remain categorized as LOW or must everything be considered HIGH impact if any of the components are classified as HIGH?
23.a	Manitoba Hydro	Disagree with proposed definition	BES Cyber System Component” definition needs to be clarified. The defining characteristics of the device should be clearly enumerated by using appropriate punctuation. Placement of semi-colons is confusing as drafted. Example: “A programmable electric device that: (a) is organized for the collection of... and (b) either: (i) responds to a BES condition or Disturbance; or ii) enables control and operation.
24.a	Luminant	Disagree with proposed definition	Better definition on "Data” should potentially be limited to the hardware that stores the data and not the data itself. This should exclude Black start radio systems and in plant personnel communications systems such as 450 Mhz radio systems. The semicolon after Disturbance should be removed.

#	Organization	Yes or No	Question 1.a. Comment
25.a	City Utilities of Springfield, Missouri	Disagree with proposed definition	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
26.a	ERCOT ISO	Disagree with proposed definition	Consider: "One or more programmable electronic devices (including hardware, software and data) designed for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
27.a	Tenaska	Disagree with proposed definition	Data integrity is out of scope because SCADA, EMS and DCS systems have software to recognize bad data. Also the display of data should be out of scope there are BES Cyber System Components that if compromised will not affect the reliability of the BES i.e. PI historian's. The Pi Historian is used to display and store data and is not used respond to a BES condition or Disturbance; or enable control and operation.
28.a	CWLP Electric Transmission, Distribution and Operations Department	Disagree with proposed definition	Data should not be included as part of a device. Communications paths should not be included.
29.a	US Army Corps of Engineers, Omaha District	Disagree with proposed definition	define term disposition [of data]
30.a	Constellation Energy Control and Dispatch, LLC	Disagree with proposed definition	Delete the term BES condition from the definition.

#	Organization	Yes or No	Question 1.a. Comment
31.a	Constellation Energy Commodities Group Inc.	Disagree with proposed definition	Delete the term maintenance and condition from the definition. The term maintenance, as used in the BES Cyber System Component statement, does not have direct impact to the reliability of the BES. Define the term disposition and describe how it applies to BES Cyber System Component.
32.a	CenterPoint Energy	Disagree with proposed definition	Disagree - CenterPoint Energy believes the definition should include a reference to an external communication connection. A disconnected cyber system component is secure. An unintended consequence of this definition may be that entities will install communication connections to isolated cyber system components to remotely manage access requirements of the standard. This defeats the benefits of isolation as a security measure. This definition as currently written would also include programmable electronic devices located in control cabinets mounted on yard equipment within the substation yard. Applying certain requirements of the current draft standards to such equipment is extremely problematic.
33.a	E.ON U.S.	Disagree with proposed definition	E ON U.S believes one or more electronic devices used exclusively to display data should not be considered a BES Cyber System Component
34.a	FirstEnergy Corporation	Disagree with proposed definition	FirstEnergy Summary Response: FirstEnergy (FE) appreciates the hard work of the CIP Standards Drafting Team in developing the version 2 CIP standards and the quick implementation of Commission directed changes reflected in version 3 CIP standards. FE strongly supports the work of the CIP SDT to develop further enhancements to the cyber security standards that improve reliability while providing clarity and certainty. Protecting and guarding against unauthorized access to cyber systems used in the protection and control of the bulk electric system is a reliability priority that FE shares. It is clear that the NERC CIP standards drafting team's fundamental approach is well-intentioned, but will result in a significant diversion of resources away from making concrete, tangible enhancements to the existing framework of cyber protections. FE

#	Organization	Yes or No	Question 1.a. Comment
			fundamentally endorses enhancements to the critical infrastructure protection standards that improve security, clarity, and certainty, but strongly believes that wholesale restructuring of the existing CIP standards is not necessary and may be counter-productive to those goals. While there are some that conclude it is not feasible to sufficiently enhance the underlying approach embodied in the existing CIP standards, these conclusions disregard the considerable investment in people, tools, and processes to address these requirements that would be abandoned in favor of an alternate formulation. Building from the existing CIP approved standards and implementation investments, while strengthening the standards to provide needed clarity and certainty offers a far expedited path to enhance cyber security, also providing greater confidence in the strength of the cyber protections in effect across the industry. A fundamental aspect the SDT proposed abandoning is the Critical Asset determination approach in favor of a wholesale impact categorization structure that introduces different terminology, concepts, and uncertainties, while offering little added clarity. We support the teams guiding principles - leveraging investments in current standards, minimizing the need for TFEs, reducing administrative overhead, etc. - however the proposed standards do not seem to practically meet the primary need for BES security. The key guiding principal for the enhanced cyber standards is clarity to which assets of the bulk electric infrastructure require cyber risk protection. The impact categorization depicted in Attachment II is a significant improvement in achieving a consistent approach for determining high impact critical assets representing the backbone of the bulk electric system. FE encourages the drafting team to focus its efforts on further developing Attachment II to obtain industry consensus on high impact assets and incorporate the work into the existing CIP-002 for consistent Critical Asset determination. To the extent essential, this work could further be integrated within the existing standards to determine another category of less-critical assets to the security of the BES, requiring respectively lesser degree of cyber security protection. Enhancing bulk electric system cyber security does not require a paradigm shift from approaches integrated into existing cyber security programs. We encourage the drafting team to maintain continuity and leverage significant industry investments in implementation of cyber

#	Organization	Yes or No	Question 1.a. Comment
			security protections undertaken over the last half-decade to achieve conformance with the CIP standards. The underlying work of the SDT reflected in the proposed CIP-010 and CIP-011 standards represent important enhancements that can, and should, be integrated with the existing CIP standard architecture, and avoid introducing new set of methodologies, definitions, and requirements that will require virtually every aspect of utility implementation to be restructured - policies, procedures, training, systems, drawings, contracts, data, compliance monitoring tools, forms, etc. These proposed changes offer little improvement in cyber security protection over what can be promptly gained by enhancing the existing standards. While the multilevel categorization is well intended, we believe the maximum security improvements can be more promptly achieved by integrating with the existing infrastructure protection requirements. In sum, FirstEnergy endorses an approach that allows for enhancements of existing implementation that affords more certainty and clarity, and avoids approaches that involve revamping the entire design of cyber protection implementation. Namely, we would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- using the standards drafting team work as an input to the enhancements of the existing standards. Enhance the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable continuity. This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure. We appreciate the drafting team's careful consideration of FE's views on the appropriate path forward in further enhancing the bulk electric system protections against unauthorized access to cyber assets. Although FE does not align with the team's overall approach we have thoroughly reviewed the proposed standards and offer constructive feedback to the specific questions asked by the drafting team. It's noted that our individual question responses in many instances do not reflect our primary position of enhancing BES cyber security in a manner that retains the framework and terminology of the existing standards. These responses are provided in order to provide clarity to the extent the concepts may be incorporated into revision of

#	Organization	Yes or No	Question 1.a. Comment
			the CIP-002 through CIP-009 standards. - - - - - - - - - - - - - Question 1.a Response: Suggested alternative definition:"BES Cyber System Component - One or more programmable electronic devices (hardware or software) relied upon to respond to a BES Contingency or Disturbance and supports control and operation of a critical BES Facility."Reasons for suggested changes: o The middle portion of the BES Cyber System Component definition is confusing and provides little value for distinguishing BES Cyber System Components from other components. The terms collection, storage, processing, maintenance, use, sharing, communication, disposition, or display do not add clarity and can be removed to simplify. The inclusion of the term "data" requires clarification. It's not clear how data can be considered a programmable electronic device. FE's proposal removes this term. The term 'BES condition' is vague and open to interpretation. We suggest use of the NERC defined term for Contingency. The team should also clarify for industry if configurable, but non-programmable devices are to be considered as BES Cyber System Components. Also it should be clear that communication media (fiber, wiring) and transport devices (SONET, Microwave, etc) installed between BES Cyber System Components are excluded.
35.a	ReliabilityFirst Staff	Disagree with proposed definition	For clarity, ReliabilityFirst suggests the following revision to the language of this requirement, ". . . (including each device's hardware, software and data). . ."
36.a	GTC & GSOC	Disagree with proposed definition	GTC and GSOC are concerned that there may be a component of a BES Cyber System which does not meet this definition of a BES Cyber System Component. If the intent is to apply a cyber security control to a BES Cyber System Component, the SDT should be careful that the definition indeed captures all of the individual devices that make up a BES Cyber System. We recommend the following definition. "A programmable electronic device (including the hardware, software and data necessary for the proper performance of its function) necessary for a BES Cyber System to perform its core functions."

#	Organization	Yes or No	Question 1.a. Comment
37.a	Matrikon Inc.	Disagree with proposed definition	I agree with this definition, but ask for a label/definition/category for those cyber systems that do not “respond to a BES condition or Disturbance; or enable control and operation” as they will exist in the field and will need to be labeled consistently across different entities/regions. Case and point, Responsible Entities could call them “Cyber System Components” or “Cyber Components” or “Discrete Cyber Assets” or “Cyber Assets”, all having the same meaning but different label for the Auditors to understand. I understand it is not a priority for the SDT to label those cyber assets not subject to NERC CIP compliance, but it would provide consistency for labeling those systems which have been evaluated, and confirmed no relationship to the Bulk Electric System.
38.a	American Municipal Power	Disagree with proposed definition	I disagree with the definition on the terms that it may introduce unnecessary or inappropriate interpretations.
39.a	Southwestern Power Administration	Disagree with proposed definition	I disagree with the proposed definition and offer a simpler one that clearly identifies what is in scope.BES Cyber System Component - A programmable electronic device that has the ability to control a BES Facility and/or process data for the real time operation of the BES.
40.a	Wolverine Power	Disagree with proposed definition	I have a concern relating to the definition of "BES generation" vs. "BES transmission”. The NERC definition for BES transmission is clear (100kV+), but NERC defers to each regional entity to define "BES generation “Acknowledgment of the regional entity's right to define what constitutes "BES generation" is important to the application of CIP-010 and CIP-011:As I read the standard, any generation determined to be "BES" in CIP-010/-011 must then automatically be categorized as "high, medium, or low" critical impact (per Attachment 2 of CIP-010). - Even the "low" impact introduces and mandates several cyber controls be in place. So my question is: (How do you objectively determine if specific generation resources really have a material effect on the BES? Some situations are obvious (reliability "must-run" resources on the grid for example) - But just because

#	Organization	Yes or No	Question 1.a. Comment
			a generation facility eventually interconnects with BES doesn't necessarily mean it's material to the BES. So the question of what constitutes "BES generation" is an important to clarify with respect to the application and ramifications of these proposed standards. Proposed Solution: Make reference to (explicitly mention in the standards) each regional entity's definition of "BES generation". In RFC's case, BES generation is defined as: (1) individual generation resources larger than 20 MVA or a generation plant with aggregate capacity greater than 75 MVA that is connected via a step-up transformer(s) to facilities operated at voltages of 100 kV or higher. This provides necessary clarity with respect to applying these standards. Generation listed as "blackstart" for a small TOP's restoration plan isn't necessarily material to the BES just because it can be argued that it eventually interconnects somehow with the BES - Clarity and bright line definition of BES generation is important to interpretation of this standard. The regional entities have provided clarification, and it should be acknowledged in these standards.
41.a	Green Country Energy	Disagree with proposed definition	I suggest adding "primary level" to the phrase enable control and operation. So that it would read enable primary level control and operation. I also request a definition of "respond to a BES condition" from a generator operator perspective.
42.a	Lincoln Electric System	Disagree with proposed definition	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
43.a	MidAmerican Energy Company	Disagree with proposed definition	MidAmerican Energy agrees with EEI's suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET,

#	Organization	Yes or No	Question 1.a. Comment
			Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the Bested terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
44.a	The Empire District Electric Company	Disagree with proposed definition	Please consider the more simple definition: BES Cyber System Component - A programmable electronic device that has the ability to control a BES Facility and/or process data for the real time operation of the BES.
45.a	US Army Corps of Engineers	Disagree with proposed definition	Please define the term disposition [of data].
46.a	Puget Sound Energy	Disagree with proposed definition	Puget Sound Energy feels that "as owned or operated by the entity" needs to be added to the definition. As the definition is currently written, the standard could be applied to telecommunication links (or the Internet) that are completely out of an entity's control to implement requirements mandated in CIP-011. Also please provide examples of how "data" is a "programmable electronic device". It seems that the hardware and software

#	Organization	Yes or No	Question 1.a. Comment
			can be programmable, but the data itself must actually reside on hardware so it's unclear how to consider it a component solely by itself.
47.a	Madison Gas and Electric Company	Disagree with proposed definition	Recommend that the word "Disturbance" be removed from the definition since the NERC definition broadens the full meaning of BES Cyber System Component. A BES condition contains both normal and emergency statuses of the BES and a disturbance is a sub component of a BES condition (taking a normal condition to an emergency condition). Disturbance reporting is currently contained in EOP-004-1 and the reporting requirements of EOP-004-1 go beyond this Project and will lead to more confusion and redundancy within the NERC Standards. Recommend that the modifier of BES be added to "or enable control and operation of the BES". Recommend changing the phrase, "display of data" to "display of data about the BES" as it is BES data and BES operation that are of interest. The new definition should read: One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of BES data; which respond to a BES condition; or enable control and operation of the BES.
48.a	Hydro One	Disagree with proposed definition	Recommend the following definition - "A programmable electronic device (including hardware and software) organized as a part of a BES Cyber System".
49.a	ISO New England Inc	Disagree with proposed definition	Recommend the following definition - A programmable electronic device (including hardware and software) utilized as a part of a BES Cyber System.
50.a	Northeast Power Coordinating Council	Disagree with proposed	Recommend the following definition - A programmable electronic device (including hardware and software) organized as a part of a BES Cyber System.

#	Organization	Yes or No	Question 1.a. Comment
		definition	
51.a	San Diego Gas and Electric Co.	Disagree with proposed definition	SDG&E recommends removing “data” and “display of data” from the definition because these terms are too vague and can potentially include many devices that should not be in-scope with these Standards (TV Monitors, strip chart recorders, digital displays, and other lower-level devices that have very little or no impact on cyber security or the reliability of the BES).SDG&E recommends the removal of the term “enable control or operation”. This seems vague and may unnecessarily roll up isolated devices (especially at substations or at Generating stations) that “enable control and operation” but have very little to do with the reliability of the BES. Many of these devices are isolated and have a very low risk of impacting the reliability of the BES.SDG&E also recommends the removal of the terms “collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data”. These terms do not help to clearly identify in-scope components and just confuse the issue as entities brainstorm all the nuances of those terms. In exchange for removing the terms identified above, we are suggesting a new revised definition for BES Cyber System Component. The centerpiece of our new suggested definition revolves around the use of a routable protocol or dialup connection, which has strong ties back to CIP-002-2 and contains terms that compliant entities are already familiar with. Suggested Revised Definition for BES Cyber System Component - One or more programmable electronic devices utilizing a routable protocol or dialup connection (including software) which is used to monitor, control, or operate the BES. In addition to revising this definition, SDG&E also recommends that the drafting team release a document (perhaps a FAQ or Guideline) that steps through examples for various entities to show what devices / facilities would be in-scope with the requirements in CIP-010. We suggest this because we believe that the current Standard as proposed will bring an enormous amount of components and systems into scope that will require substantial resources to be compliant with the Standard. Will the reliability of the BES increase by the same substantial amount?
52.a	Regulatory Compliance	Disagree with	Some components such as the display of data may not impact real time operation. More

#	Organization	Yes or No	Question 1.a. Comment
		proposed definition	clarification is needed or strike the display of data from the definition.
53.a	IRC Standards Review Committee	Disagree with proposed definition	Some devices may meet the definition of BES Cyber System Component, particularly "enable control and operation" but have little to no impact to the BES if unavailable or compromised because operators may have alternative means to provide the same functionality. Is the intent of this phrase in the definition to expand the applicability of the term to components that are not related to BES condition or Disturbance? Or is it meant to apply only to those components that respond to BES condition or Disturbance?
54.a	Network & Security Technologies Inc	Disagree with proposed definition	Suggest striking "data" from the proposed definition. Cyber Systems and/or their components perform various operations with data (create it, store it, modify it, send or receive it, etc.), and data is of course fundamental to reliable, computer-aided or controlled operation of the BES, but it is not a "programmable electronic device."
55.a	Entergy	Disagree with proposed definition	Suggest: "or more" should be stricken; 'component' should be singular - a discrete unit. "Or more" is appropriate in the BES Cyber System definition below.
56.a	Allegheny Power	Disagree with proposed definition	Suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System

#	Organization	Yes or No	Question 1.a. Comment
			Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
57.a	EEI	Disagree with proposed definition	Suggested alternative definition: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Alternatively, BES Cyber System could be defined before BES Cyber System Component. This would follow a top town approach. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage,

#	Organization	Yes or No	Question 1.a. Comment
			maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed. SUGGESTION: Reorder positions to place "BES Cyber System" prior to "BES Cyber System Component", this follows a top down approach. BES Cyber System - A system performing one or more BES functions identified in CIP-010 Attachment 1 and which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, adversely impact the real-time operational control of the BES.BES Cyber System Component - One or more programmable electronic devices that are a component of a BES Cyber System and which if rendered unavailable, degraded, compromised, or misused would adversely impact a BES Cyber System. Control Center - A location where one or more BES Cyber Systems are used to perform BA, RC, or TOP functions for generation Facilities or Transmission Facilities at multiple sites. Also consider removing the word communications. This would include any connection via leased lines or other third party data circuits.
58.a	Duke Energy	Disagree with proposed definition	Suggested clarifying change as follows: "One or more electronically programmable devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
59.a	Alberta Electric System Operator	Disagree with proposed definition	The AESO would like to see a more detailed definition of "enable control and operation" and a definition of "BES condition".
60.a	APPA Task Force	Disagree with proposed definition	The APPA Task force disagrees with the current definition and would like to point out areas where it can be improved. Foremost, we feel the whole standard revolves around the concept of routable protocol. Since this is a common theme of a number of the requirements we feel this should be included in the definition. Also we think the current definition tries to cover a laundry list of functions which complicates the definition. We provide the following edited version for the drafting team's

#	Organization	Yes or No	Question 1.a. Comment
			consideration: BES Cyber System Component -A programmable electronic device connected via routable protocol, which responds to a BES condition or Disturbance, or enables control and operation of the BES. If the drafting team does not use this version we at least request that adding “connected via routable protocol” be included in some manner in the definition that is used.
61.a	Wolverine Power	Disagree with proposed definition	The concepts of "BES" and "critical", as they relate to generation, need to be revisited and clarified -For example - A BES generator, that is used only occasionally, for peaking purposes, and is not black start capable, may logically be declared as "non critical" using the current NERC CIP guidelines - but under these proposed standards, as I read them, this example might be forced to be considered as "low impact".(low criticality vs. not critical)The existing CIP standards allow for a logical separation between "BES and Critical" (i.e. just because a generator is BES doesn't automatically mean it's critical to the BES - how it's used should be taken into consideration) Under these proposed standards, as I read them, any generation resource identified as BES, automatically must be characterized as "low impact" at a minimum. I believe there should be some language in the standard that 1) takes into account the regional entity's right to define what constitutes BES generation; and 2) Doesn't force a "low impact" by default on any and all "BES" generation, without due consideration of its actual use and true impact on the BES.
62.a	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree with proposed definition	The current standard limits its applicability to those systems with routable protocols or dial-up access. That limits the applicability of the CIP standards to those systems that are accessible and therefore vulnerable. This proposed standard will impose the CIP requirements on all programmable equipment regardless of its accessibility to external forces. A cyber system inside a generator accessible only to generator staff is as critical to its function as any pump or valve. The security measures safeguarding the pump and the valve should also be sufficient for the cyber system. Only those cyber systems accessible to the outside world require additional, special security requirements. Similar comments were made by many parties in response to the definitions in the proposed

#	Organization	Yes or No	Question 1.a. Comment
			version 4 CIP standards.
63.a	Southwest Power Pool Regional Entity	Disagree with proposed definition	The definition as written could be read to imply that data is a BES Cyber System Component. Data is not a programmable electronic device; however data can reside on a programmable electronic device. The definition should be clarified to make it clear to the reader that the programmable electronic device includes any software and/or data residing on the hardware. Also, consider changing “or enable control and operation” to “or enable control, operation, and/or situational awareness.”
64.a	MWDSC	Disagree with proposed definition	The definition is confusing with disconnected phrases and will be subject to many interpretations. What’s the difference between a “condition” and a Disturbance? The NERC Glossary defines Disturbance as 3 events which should cover all relevant conditions. The proposed definition may be interpreted to include a condition on a local BES system which will not create a Disturbance to an interconnected system. For example, a relay for a transmission/distribution bank breaker may operate and drop the distribution voltage load connected to that BES substation, but not create any Disturbance to other systems. The term "control and operation" was changed from prior draft to "monitoring and control" -see Attachment I under CIP-010. Also, it is unclear who controls and operates the component. In the extreme, a smart grid meter on a distribution circuit could be a “programmable electronic device” which responds to or enables control of a BES condition by reducing or dropping load. Suggest changing definition as follows: "BES Cyber System Component - One or more programmable electronic devices connected to the BES (including hardware, software and data), organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data, and which respond to a BES Disturbance affecting an interconnected BES system or enable monitoring and control of the BES by a Transmission Operator, Generator Operator, or Balancing Authority."
65.a	USACE HQ	Disagree with proposed	The definition is still too broad. The definition includes “software and data” as devices, but when someone thinks of a device usually it is a physical component. I think the intended of the team is to state that the software and the data must be included as part

#	Organization	Yes or No	Question 1.a. Comment
		definition	of the device definition, therefore I suggest changing the definition from a "programmable electronic devices (including hardware, software and data)" to "programmable electronic devices (including its components such as hardware, software and data)". Also, the definition is broad enough that test environments and maintenance devices can be included in the definition. CIP-011-1, page 22, states that "devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System". I suggest that the exclusion of devices "not permanently connected to (the) BES Cyber Systems" be explicitly present in the definition of BES Cyber System Component. Lastly, I suggest that all the definitions, in both CIP-010-1 and CIP-011-1 be present together to make it easier for the reader to understand all the new language introduced to the standards
66.a	Kansas City Power & Light	Disagree with proposed definition	The definition is too broad regarding the application of the data used by programmable devices. The proposed definition would include devices used for system analysis or system maintenance with historical data (e.g. Disturbance Monitoring Equipment (DME)). The important considerations are for those devices for the processing and use of data in the real time control of the BES. Recommend modification of the current definition to: One or more programmable electronic devices (including hardware, software and data) organized for the processing and use of data for the purpose of control and operation of the BES.
67.a	US Bureau of Reclamation	Disagree with proposed definition	The definition needs to clarify that the phrase "or enable control and operations" applies only to Cyber System Components that enable the control or operation of BES Assets. It will also need to define the term BES Assets.
68.a	Exelon Corporation	Disagree with proposed definition	The definition should only contain elements that are directly associated with obtaining and using data in support of reliable real-time operations or a device that would automatically respond to an adverse condition on the BES. Specifically the elements in the proposed definition of storage, maintenance, sharing and disposition should not be included. The display of data is also not needed as the display of data would be covered

#	Organization	Yes or No	Question 1.a. Comment
			by the "use" element. The definition needs to be more definitive with the term "programmable electronic devices" and their potential to impact the BES. The definition should consider whether a device can be controlled or operated via remote communication. Disturbance (as defined in the Glossary of Terms Used in NERC Reliability Standards April 20, 2010) is too vague and casts too wide a net and is not in synch with EOP-004. The term "BES condition or disturbance" needs to be clarified. Exelon has a concern that this definition may be interpreted differently in each region.
69.a	Con Edison of New York	Disagree with proposed definition	The Drafting Team (DT) should not include collection, storage, maintenance, use; sharing, communication, disposition, and display of data in the definition because these components cannot respond to a BES condition and may add ambiguity to the definition. By including these words, the Standard is implying that company networks outside of the EMS (e.g. PI) may be included as BES Cyber Systems. Suggested alternative definition: "Any microprocessor-based programmable electronic device used to enable control and operation of a BES element."
70.a	Electricity Consumers Resource Council (ELCON)	Disagree with proposed definition	The existing standard applies to systems with routable protocols or dial-up access. That limits the application of the CIP standards to systems that are accessible and therefore vulnerable. The proposed new standard will impose the CIP requirements on all programmable equipment regardless of its accessibility by external threats. Only those cyber systems accessible to the outside world require special security requirements.
71.a	SCE&G	Disagree with proposed definition	The language "enable control and operation" needs to be better defined. What constitutes control?
72.a	Indeck Energy Services, Inc	Disagree with proposed	The phrase "which respond to a BES condition or Disturbance" doesn't differentiate a component that takes action directly because of the BES condition or Disturbance and one that takes action when told to do so following a BES condition or Disturbance. For example, an under-frequency relay will take action on its own (e.g. trip) upon measuring

#	Organization	Yes or No	Question 1.a. Comment
		definition	the frequency and time corresponding to its setpoint, whereas, a generating unit without a governor will increase generation when the ISO, RTO or TO requests it to do so following the BES condition or Disturbance. The second system shouldn't be categorized as a BES Cyber System Component based on its action following a BES condition or Disturbance. --------- [suggestion] "One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which independently respond to a BES condition or Disturbance."
73.a	Oncor Electric Delivery LLC	Disagree with proposed definition	The purpose of a "component" is to collect, store, process, etc DATA. Data should not be included in the specification of a "component". It should read, "One or more programmable electronic devices (including hardware and software) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation."
74.a	LADWP	Disagree with proposed definition	The term "organized" seems to broaden the scope of a BES Cyber System Component to any device that may not be utilized but could be utilized in the BES system. A clearer definition needs to be made.
75.a	American Electric Power	Disagree with proposed definition	The term "programmable electronic devices" is general and vague. For example, based on this definition it is not clear how it will align with transmitters and other microprocessor systems. AEP suggests that the drafting team develop a definition that provides more clarity as to what is to be considered in scope. AEP suggests using the wording of NIST SP800-82 sections 2.3.1 and 2.3.2 to clarify the control system components that need to be evaluated for security controls.
76.a	Public Service Enterprise Group companies	Disagree with proposed	The text in brackets "(including hardware, software and data)" is not clear. These items are not types of "programmable electronic devices". Does a specific piece "software" or "data" collection constitute a "BES Cyber System Components"? This text needs to be

#	Organization	Yes or No	Question 1.a. Comment
		definition	dropped or a clearer definition is required.
77.a	Minnesota Power	Disagree with proposed definition	This definition is generally acceptable, with clarification or correction regarding the following items: o What if the device is not programmable, rather defined to perform one function (i.e., coded in firmware)? These types of devices still could have security flaws. What is meant by “disposition” of data? Disposition of data is typically a maintenance function performed after-the-fact which would not have a real-time impact on the BES. There are corporate system which ultimately receive, display and/or act upon data pertaining to the BES. These are not for real-time operations, and should immediately be recognized as out of scope. This definition should reference “real-time operations” or “BES Reliability” to clarify the intended scope. Minnesota Power recommends the following revised definition:"One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, or display of data which, in real-time, respond to a BES condition or Disturbance or enable control and operation."
78.a	Ameren	Disagree with proposed definition	This definition is overbroad and potentially brings in an inappropriate number of devices that should be excluded from the scope of this definition, e.g. display terminals, personal cell phones, pagers etc. The last sentence "which respond to a BES condition" is too encompassing, and the term Disturbance is also. Also, if “communication” devices are going to be included in this definition, then communication devices need to be more precisely defined. The definition of BES Cyber System Component includes “disposition.” This phrase should either be defined more precisely or removed.
79.a	Midwest ISO	Disagree with proposed definition	This definition is overly broad and seems to miss the point that the information technology is there to support the operation of the BES and not vice versa. For example, collection and storage of data does not impact the operation of the BES and should not even be considered unless the facility can be used to control or manipulate the operation. Furthermore, what does it mean to respond to a BES condition? Suggest modifying the definition to: One or more programmable electronic devices (including

#	Organization	Yes or No	Question 1.a. Comment
			hardware and software) organized to enable control, operation and protection of equipment.
80.a	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree with proposed definition	This is a vast improvement over "Bulk Electric System Subsystem," and agrees with the focus on the cyber system up front rather than round about. However, there is room for further improvement. The present proposed definition can include programmable relays with no network connection at all - serial or addressable - to cell phones used to receive SCADA alarms. The main focus of the Standard is to protect BES Cyber Systems that are vulnerable to network/Internet based attack, or infection from malicious software. Secondary is the need for physical protection; however, all critical facilities whether cyber or not in nature need physical protection. Therefore in light of this, restricting to components that are vulnerable to remote attack via a network, the Internet, or the inadvertent infection of malware is advised. It should be recognized that not all programmable electronic devises are subject to "cyber attack," and should be excluded. "including hardware" may fail to clarify what is included; does this include a network and supporting equipment connected to the BES Cyber System Component such as a printer, or does it imply only the programmable electronic device itself? The use of "respond to" implies automatic operations the BES Cyber System performs and the additional qualifiers "control and operation" implies programmable equipment that only supplies monitoring data of the BES is outside the CIP scope. This does not appear to cover the required need for BES operator situational awareness of the electrical condition of the BES, and partially negates the BES Cyber System definition below.CIP-011-1 R26 considers maintenance devices to not be part of a BES Cyber System. These devices should be excluded from the proposed definition to be consistent.CIP-011-1 R11 considers devices used to remotely access BES Cyber Systems to be external to those BES Cyber Systems. These devices should be excluded from the proposed definition to be consistent.
81.a	Pepco Holdings, Inc. - Affiliates	Disagree with proposed	We agree with EEI's comments including the position on software and data. In addition, there seems to be a potential for confusion by including "one or more" in the definition. Because there does not seem to be a clear distinction between BES Cyber System

#	Organization	Yes or No	Question 1.a. Comment
		definition	Component and a BES Cyber System, it would seem like a BES Cyber System Component could qualify as a BES Cyber System.
82.a	We Energies	Disagree with proposed definition	We Energies agrees with the EEI Suggested alternative definition and explanation: BES Cyber System Component - One or more programmable electronic devices (including hardware) organized for the processing, or display of BES operating status or condition; which respond to a BES condition or Disturbance; or that enable BES control and operation. The following elements are excluded from this definition: o Voice Communication systems media (fiber, wiring, etc.) and transport devices (SONET, Microwave Equipment, etc.) installed between BES Cyber System Components as long as all access points are controlled by firewall devices. Explanation:"Software" has no function or purpose in the absence of an electronic host upon which it operates. To the degree that it is appropriate to identify controls or security objectives associated with software operating on [hardware] BES Cyber System Components, requirements should address software issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES."Data" is an extremely broad term that has very different meanings depending on the specific context within which it is used. To the degree that it is appropriate to identify controls or security objectives associated with data used for real time BES system operations, those requirements should address data integrity, availability, or confidentiality issues specifically, rather than generally which may lead to inappropriate and ineffective controls which will not enhance to reliability of the BES. The terms storage, maintenance, disposition do not add clarity to the definition of BES Cyber System Component, and should be removed.
83.a	Garland Power and Light	Disagree with proposed definition	We have concerns about data being included in the definition - Many of the CIP requirements are difficult to document or comply with for the data.

#	Organization	Yes or No	Question 1.a. Comment
84.a	Southern Company	Disagree with proposed definition	We recommend the following definition: One or more programmable electronic devices that are a component of a BES Cyber System and which if rendered unavailable, degraded, compromised, or misused would adversely impact a BES Cyber System. This definition should be moved to after the definition of BES Cyber System to reflect a top-down approach. If the list of functions is found to be necessary, communication should be removed or, at least, limited to communication outside the BES Cyber System.
85.a	Alliant Energy	Disagree with proposed definition	We think the existing definition is too broad and propose the following: One or more programmable electronic devices (including hardware and software) organized to enable control, operation and protection of BES equipment.
86.a	MRO's NERC Standards Review Subcommittee	Disagree with proposed definition	We think the existing definition is too broad and propose the following: One or more programmable electronic devices (including hardware and software) organized to enable control, operation and protection of BES equipment.
87.a	Constellation Power Source Generation	Disagree with proposed definition	What is the definition of the term “BES condition”? It is not a term in NERC’s Glossary of Terms. It needs a local definition much like other terms have been defined in these standards. Using the definition proposed for a BES Cyber System Component, is the intent to include electronic meters such as Nexus Meters? They do not respond to a BES condition, but they do display data. Constellation’s interpretation would be that they are out of scope, but that may not be the intent of the SDT.
88.a	Verizon Business	Disagree with proposed definition	The definition should be specific to the Bulk Electric System to ensure that it does not include generation facilities used on distribution systems or non-BES facilities. This change could be accomplished by adding to the end of the sentence "... on the Bulk Electric System (>100 kv)."

1.b. BES Cyber System — One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.

Summary Consideration:

Many conmmentors observed that the definition of the 15-minute window was too ambiguous. Others observed that a 30-minute window would be more in alignment with other reliability standards. Many commenters observed that the impact was too vaguely described in the definition, and the scope was too broad.

The SDT has carefully reviewed the 15-minute window and has concluded that 15 minutes was more representative of a real-time impact. Some reliability standards cite 30 minutes as recovery times, others cite 15 minutes. The SDT believes that a 30 minute window may include more systems that would not have a "real-time" effect on the reliability of the BES. The SDT has shifted the BES impact aspect of the definition of BES Cyber Systems to the definition of BES Cyber Assets, with clearer definitions of the impact, with respect to "BES Reliability Operating Services", and specific reference to BES "real-time" reliability operations.

The new definition of **BES Cyber System** is:

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

#	Organization	Yes or No	Question 1.b. Comment
1.b	BGE	Agree	1.a and 1.b should be reversed.
2.b	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the definition but believes that the definition can be improved significantly. FMPA offers the following simpler definition:"One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a Disturbance to the BES, or restrict control and operation of the BES within 30 minutes."For the following reasons: (i) see comments to Question 2 for time considerations; and (ii) including that phrase loss of situational awareness is superfluous since it restricts control and operation of the BES and is therefore included in that term.

#	Organization	Yes or No	Question 1.b. Comment
3.b	Puget Sound Energy	Agree	Generally agree, however it is unclear how to use the 15 minutes very meaningfully and how that will be tested in an audit.
4.b	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
5.b	Green Country Energy	Agree	Please define "affect situational awareness"
6.b	Reliability & Compliance Group	Disagree	: There needs to be more clarification about what it means to “restrict control and operation.” If you lose backup control, does this restrict control and operation if you still have primary control? Also, provide a definition of situational awareness in the standard at this point and capitalize the term.
7.b	Oncor Electric Delivery LLC	Disagree	“Systems” are categorized as high, medium and low, entities will tend to identify “Cyber System” at the lowest level possible. We need more clarity (white paper) to assist in how utility equipment should be identified as components or systems.
8.b	Indeck Energy Services, Inc	Disagree	1) The phrase “if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause” is too broad with the word “could”. The proper standard should be “is highly likely to cause.” 2) Situational Awareness is defined as the state of the BES. If this means that it includes systems and data used in the State Estimator, then it should specify that. The more specific the definition, the more certainty that BES ALR will be assured. 3) In FERC Order 706, NERC was required to “provide sufficient guidelines to inform generation owners and operators on how to determine whether it should identify a facility as a critical asset.” The only guideline that this definition provides is that the Cyber System could cause a disturbance. Spread across the nine Functions in Attachment I, this is patently incomplete as guidelines. For each of the Functions, some basis for a risk assessment should be outlined. [suggestion] “As to function Controlling Voltage (Reactive Power), any BES facility (asset) capable of providing <100 MVARS is not a BES Cyber Asset as to this function.” 4) [suggested replacement language] "As determined through the application of the Registered

#	Organization	Yes or No	Question 1.b. Comment
			Entity's risk based assessment methodology, one or more BES Cyber System Components which, if rendered unavailable, degraded, compromised, or misused, is highly like to cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES."
9.b	Progress Energy (non-Nuclear)	Disagree	1. Need a better statement of what 'within 15 minutes' means. Is 15 minutes considered real time operation? Most disturbances will occur in milliseconds. Is there a basis for 15 minutes? A malicious code could lie dormant for extended periods of time, but if activated may have an immediate impact. The term misused is very subjective and may need clarification. The 15 minute window may be good in that it possibly excludes equipment such as circuit breaker hydraulic, pneumatic and gas systems which may cause a breaker to be removed from service but not within 15 minutes. 2. With the 15 minute definition and using organized subsystem concept from 1.a. we can design Cyber (sub)Systems' delineation to effectively minimize impact on BES (see question 7 below). Limit Medium, High impact to a select few subsystems with the rest Low impact. Alternatively the entire plant control system would be viewed as one large Cyber System (High Impact) with the resultant full CIP requirements.3. Rules regarding redundancy need to be clearly defined. The 15 minute window brings redundancy into the picture.4. Need clarification of the terms 'compromised' and 'misuse'.5. Need to know if this would include DCS networks that do "batch" (non-continuous) type control. Some examples would include coal/limestone/gypsum conveying, limestone slurry processing, etc. These processes have inherent storage capabilities that far exceed the 15 minute rule.
10.b	Consultant	Disagree	1. The term would appear to imply that the "one or more BES Cyber System Components" perform a function related to the BES, for example, voltage control, generation control, transmission control, etc. The definition does not appear to address a "Cyber System", it appears to address just a "pile of components". If the answer is just the impact as it applies to a "pile of components", then this term would seem unnecessary as the "pile of components" is covered by the BES Cyber System Components term. It would seem that this definition should distinguish between

#	Organization	Yes or No	Question 1.b. Comment
			components, such as multiple desktop computers and servers as individual devices and their installed software (BES Cyber System Components), and the collection of those components networked and programmed to function as an Energy Management System (BES Cyber System).2. This clarification then raises the question whether the threat ("degraded, compromised, or misused") is a threat to components or a threat to systems. If the component is threatened then the system is threatened, but is there a mechanism to threaten the system without threatening the components? 3. This clarification would have an impact on the methodology for identifying affected assets.
11.b	Entergy	Disagree	A) How is “restrict” defined? How will this be audited? Suggest: Consider deletion B) Many things can “affect” situational awareness of the BES? Suggest “could...adversely affect.” C) How much loss of situational awareness does it take to adversely affect the BES? We lose it all the time and keep on running (e.g., temporarily using state estimators) Suggest: Consider deletion D) How much of the BES is at issue? Suggest: “...could, within 15 minutes, cause a Disturbance in that part of the BES falling under the aegis of the Responsible Entity.”
12.b	Nuclear Energy Institute	Disagree	Agree with the exception that: The word “could” is ambiguous. Propose changing could to would. Additionally, this definition does not maintain alignment with the definition of “reliable operation” provided in Section 215 of the Federal Powers Act: “The term “reliable operation” means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” The definition of BES Cyber System should be revised. An acceptable definition would be:”One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.” Lastly, it should

#	Organization	Yes or No	Question 1.b. Comment
			also be clarified that a single facility may have BES Cyber Systems that have different impact categorizations. Upon initial read, it would seem that if the one system in a generating station has a power capability of 2,000MW, then every BES Cyber System at the station is High Impact, which is inappropriate.
13.b	GTC & GSOC	Disagree	Although we appreciate that it is extremely difficult to define this concept, the current definition is too expansive. The phrase "affect situational awareness of the BES" could be interpreted to include the loss of a single status point. Such a minor outage would "affect situational awareness of the BES" but only to a trivial extent. The same could be said with respect to control. We suggest an alternative below. In addition, CIP 010 creates the definition above and then qualifies it in R1 to include only the BES Cyber Systems that "enable one or more functions defined in CIP 010 -1 Attachment I". But CIP 011 has no such qualification (except in its purpose statement), so in theory CIP 011 could apply to a more expansive set of assets than CIP 010. We recommend that the qualifications in R1 be incorporated into the definition. The clarification regarding maintenance devices that is currently in the local definition for maintenance devices (R26) should be part of this definition. Finally, the term "owned" is too narrow; theoretically an entity could absolve itself of all CIP compliance responsibility by leasing its systems. As noted in response to question 10 below, perhaps the concept of “responsible for” would be more appropriate than “owns.” We recommend the following definition: One or more BES Cyber System Components which: 1) Performs one of the following functions-Dynamic Response-Balancing Load and Generation-Controlling Frequency (Real Power-Controlling Voltage (Reactive Power)-Managing Constraints-Monitoring & Control-Restoration of BES-Situational Awareness-Inter-Entity Real-Time Coordination, and 2) if rendered unavailable, degraded, compromised, or misused, could, within 15 minutes: (a) cause a disturbance to the BES; (b) restrict control and operation of the BES to the extent an entity can no longer fulfill its obligations under Reliability Standards; or (c) degrade situational awareness to the extent that an entity can no longer maintain an accurate view of the operational status of the portion of the BES it is responsible for. 3) Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered

#	Organization	Yes or No	Question 1.b. Comment
			part of a BES Cyber System.
14.b	BCTC	Disagree	BCTC recommends the following aspects of this definition be revisited: Â reword "within 15 minutes" to "15 minutes or less" the 15 minute threshold is considered adequate for high impact systems but feel that the threshold would not be the same for medium and low impact systems; for low impact systems, for example, the threshold could be as high as 24 hours before any potential impact to the BES would be realized.
15.b	Network & Security Technologies Inc	Disagree	Believe the 15-minute threshold, while intended to distinguish systems required for and/or affecting real-time ops from others, could have a number of unintended consequences. Entities inclined to "game the system" could declare none of their cyber systems would impact the BES if lost or compromised for at least 20 minutes. How would such a claim be verified or disproven? Moreover, wouldn't a 15-minute threshold compel the establishment of cyber security incident response and/or recover plans with an often unrealistic time to complete of 15 minutes? That this is a difficult problem is understood - at a minimum the SDT might consider adding language to CIP-010 and 011 indicating this definition should not be interpreted as requiring a 15-minute recovery time interval for BES Cyber Systems.
16.b	Platte River Power Authority	Disagree	BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a real-time deadline to be missed resulting in a Disturbance to the BES, or restricting control and operation of the BES, or affecting situational awareness of the BES.
17.b	Minnesota Power	Disagree	BES Cyber System should be defined as "physical or logical set of one or more BES Cyber System Components which if rendered unavailable, degraded or compromised, could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES or restrict control and operation of the BES."
18.b	WECC	Disagree	Change "affect situational awareness" to "loss of situational awareness". Also is Situational Awareness defined? The 15-minute criterion seems arbitrary and unneeded.

#	Organization	Yes or No	Question 1.b. Comment
			The ability to negatively impact the BES is an attribute that either exists or does not regardless of time factors. The time element should be removed.Bulletizing the list of impacts would better format the definition.The following rewrite is proposed; BES Cyber System - One or more BES Cyber System Components deployed for: The control and operation of the BES; or Collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data used in control and operation decision making for the BES. These systems, if rendered unavailable, degraded, compromised, or misused could cause one or more of the following; A Disturbance to the BES; or Restrict control and operation of the BES; or o Affect situational awareness of the BES.
19.b	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
20.b	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree	Comments to Question 1.a above apply here also. Additionally, this definition would be difficult to apply for many entities. For example, how would a GOP determine if a problem at a generation plant would, within 15 minutes, cause a Disturbance to the BES if a BES Cyber System is rendered unavailable, degraded, compromised, or misused? In most cases, our experience with plant trips, equipment malfunctions and forced shoutdowns has indicated no effect on the interconnected grid.Guidance will be needed on how entities who do not operate the BES and do not have access to BES studies can determine if their facility will cause a Disturbance to the BES within 15 minutes when a Cyber System is unavailable, degraded, compromised, or misused.
21.b	ERCOT ISO	Disagree	Comments: The 15 minute requirement does not align to the other reliability standards. Recommend changing to 30 minutes to align with the EOP standards.
22.b	Southwest Power Pool Regional Entity	Disagree	Consider changing “One or more BES Cyber System Components...” to “One or more logically related BES Cyber System Components...” Also, is the term “Disturbance” well understood? The three definitions found in the NERC Glossary of Terms (April 20, 2010) use vague terms that may be open to interpretation by the reader. Similarly, the term “affect situational awareness” is sufficiently vague to be unclear exactly what is meant.

#	Organization	Yes or No	Question 1.b. Comment
			Without precise definitions, the entity and auditor may have different interpretations of the terms.
23.b	Constellation Energy Commodities Group Inc.	Disagree	Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.Suggest that the time horizon be changed to within 10 minutes to remain consistent with the Area Control Error requirements. As stated in NERC documentation: DCS measures if a control area is meeting its reserve requirements. These reserves include contingency reserve and regulating reserve. The control area must: 1) recover from the contingency and 2) regulate to load changes over the ten minutes, but the control area need not correct control error that existed before the contingency.If the control area or reserve sharing group recovers ACE to zero or to the level of ACE prior to the first contingency within ten minutes of the start of the second contingency then count two contingencies as recovered 100% within 10 minutes. BAL-001-0.1a - Real Power Balancing Control PerformanceIn order to ensure that the average ACE calculated for any ten-minute interval is representative of that ten-minute interval, it is necessary that at least half the ACE data samples are present for that interval.
24.b	Constellation Energy Control and Dispatch, LLC	Disagree	Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon

#	Organization	Yes or No	Question 1.b. Comment
			to directly operate equipment.
25.b	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes this definition is ambiguous. The NERC glossary definition of "Disturbance" is very broad and "affect situational awareness" is also ambiguous. In addition the word “could” as used in “...could, within 15 minutes, cause a Disturbance...” is problematic. “Could”, under what circumstances or what system conditions? Further clarification is required.
26.b	Turlock Irrigation District	Disagree	Disagree because this definition would include communication systems which are currently exempt from the CIP Standards and would therefore represent a major expansion of the cope of the CIP Standards. Was this the intention of the SDT?
27.b	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Disturbance has no metrics in its definition: “1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system. 3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.” Therefore any “unplanned event that produces an abnormal system condition” on the BES must be included. Coupled with the broad definition of BES Cyber System Component, almost all programmable electronic devices will be included. Consider the following: loss of a programmable relay and its redundant backup will create the loss of protection on the BES facilities it is assigned to; these relays are not networked with any other cyber systems. The loss, say from malicious physical tampering from a disgruntled employee within the substation, is the unplanned event; and the resulting loss of BES transmission protection is the abnormal system condition. Therefore, it appears that the programmable relays must be included as a BES Cyber System even though the only way to compromise these components is through direct physical contact.If the definition of BES Cyber System Component is expanded to include monitoring ability, “situational awareness of the BES” should be clarified to encompass the electrical status of the BES. Otherwise, situational awareness can include video surveillance and security equipment that is programmable. Security systems should not be considered except where they help protect Medium or High Impact BES Cyber System Components and BES facilities. The cell phone

#	Organization	Yes or No	Question 1.b. Comment
			mentioned in 1.a. above is a BES Cyber System if it displays BES alarms. CIP-011-1 R26 considers maintenance devices to not be part of a BES Cyber System. These devices should be excluded from the proposed definition to be consistent. CIP-011-1 R11 considers devices used to remotely access BES Cyber Systems to be external to those BES Cyber Systems. These devices should be excluded from the proposed definition to be consistent.
28.b	National Grid	Disagree	Do not have a clear understanding of the "within 15-minutes" interval to have an impact on the system. It appears that this clause applies only to control operations such as opening and closing of a breaker. In substations where protection and control are integrated it would be possible to make changes that will take longer than 15 minutes to impact the BES. What type of contingencies will be considered for the 15 minute time horizon? (n-1, n-2 or none). Also, many of the cyber systems are programmable devices. The cyber security could be compromised in real time and the detrimental effect can be achieved after a programmed time interval. This issue requires to be addressed in the definition. There is also no link between attachment I and definition of BES Cyber System. Suggest tying attachment I with definition of BES Cyber System. National Grid proposes the following definition: One or more BES Cyber System Components which execute(s) or enable(s) one or more functions essential to the reliable operation of the BES and which, if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness.
29.b	Dominion Resources Services, Inc.	Disagree	Dominion supports the inclusion of "within 15 minutes". It is important to establish a reasonable boundary condition for real-time or near real-time effects of the BES Cyber System and 15 minutes provides adequate time for the effects to be mitigated to prevent further harm to the BES. In addition, Dominion proposes to replace the phrase "or affect situational awareness of the BES" with "or affect BES situational awareness of one or more of the following: Balancing Authority, Transmission Operator, Reliability Coordinator." This modification is reflected in the revised definition below: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable,

#	Organization	Yes or No	Question 1.b. Comment
			degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES; or restrict control and operation of the BES; or affect BES situational awareness of one or more of the following: Balancing Authority, Transmission Operator, Reliability Coordinator.
30.b	E.ON U.S.	Disagree	E ON U.S. believes the term "affect situational awareness" is overbroad. E.ON U.S. suggests that this term should be rewritten as "degrade situational awareness." Also, "Unavailable" is not clearly defined. E.ON U.S. believes that it would be helpful if one could determine "no impact" assessments
31.b	Exelon Corporation	Disagree	Exelon suggests that the time period should not be stated in specific minutes. The standard should be revised to "One or more BES..., or misused could, without sufficient time to take mitigating action, cause a disturbance to the BES,..."
32.b	Progress Energy - Nuclear Generation	Disagree	For nuclear purposes the use of the word "component" conflicts with the definition in 1a. A system contains components rather than a component being a system.
33.b	USACE - Omaha Anchor	Disagree	Further clarify Disturbance to the BES - potentially consider "negative Disturbance"
34.b	USACE HQ	Disagree	Given that BES Cyber System is based on the definition of BES Cyber System Components, which I disagree with, I must also disagree with this one. Furthermore, the use of a time limit to represent real-time should not be present given that is lacking documentation support for the number. Either introduce a definition for real time for CIP purposes or provide support for the risk-informed dentition of using 15 minutes as the limit.
35.b	Southwestern Power Administration	Disagree	I disagree with the proposed definition and offer a simpler one that clearly identifies what is in scope.BES Cyber System - A collection of one or more BES Cyber System Components which control a BES Facility(s) and/or process data for the real time operation of the BES. To define the scope of applicability for the CIP standards, real time is considered to be the operational time horizon of approximately 15 minutes.

#	Organization	Yes or No	Question 1.b. Comment
36.b	The Empire District Electric Company	Disagree	I disagree with the proposed definition please consider the simpler one that clearly identifies what is in scope.BES Cyber System - A collection of one or more BES Cyber System Components and associated communication network(s), which control a BES Facility(s) and/or gather data for the real time operation of the BES.
37.b	Kansas City Power & Light	Disagree	Including "within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" in the definition provides a difficult set of parameters that encourages issues with interpretation of what would constitute the situations under which "within 15 minutes" applies, as well as, what constitutes "restricted control or generation"? It is understood the Drafting Team is trying to capture the essence of those systems that have a real-time impact on the BES, however, it is recommended to limit the scope of the applicable "BES Cyber System" to those systems that support facilities that are identified as critical to the reliability of the transmission grid determined by regional system study. Recommend the following definition for consideration: One or more BES Cyber System Components that provide support for facilities that have been identified as critical to the reliability of the BES.
38.b	Ingleside Cogeneration, LP	Disagree	Ingleside Cogeneration, LP believes that this definition is still too vague to make a determination of whether a system meets the threshold of a BES Cyber System and can be assigned a "No-Impact" rating. This is in stark contrast with the "bright line" delineation between High Impact systems and Medium Impact systems provided in Attachment II of CIP-010-1. The components of the definition in question are "restrict control and operation of the BES" and "affect situational awareness of the BES". Both seem to be Control Center concepts and could be interpreted to mean that any system supporting multiple generation or transmission facilities at multiple locations would automatically carry at least a "Low-Impact" rating. However, this does not speak to the associated generation or transmission facilities that may be "No-Impact" if a cyber intrusion cannot cause a Disturbance - a term which is very well defined in EOP-004-1. Ingleside's concern is that recent rulings by FERC concerning the definition of the BES

#	Organization	Yes or No	Question 1.b. Comment
			and the applicability of PRC-023-1 to facilities under 200 kV, indicate they are pushing a stricter level of adherence to Reliability Standards across the board. If this continues, Functional Entities with “No-Impact” systems once considered compliant with CIP-010-1, may be considered non-compliant at a future date. This could lead to the assessment of violations and fines, even though the Standard has not changed.
39.b	Emerson Process Management	Disagree	It could be more appropriate to state that the unavailable component(s) can not be recovered within 15 miuntes.
40.b	Bonneville Power Administration	Disagree	It is not clear that this definition limits the scope and applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems as indicated in Attachment I and Question #2 of this comment form. Situational Awareness is too broad and all the commas in the definition can lead to numerous interpretations of the sentence. Recommend changing the definition to the following: "One or more BES Cyber System Components which if rendered unavailable, degraded compromised, or misussed could, within 15 minutes: (1) cause a Disturbance to the BES; or (2) restrict real-time control and operation of the BES; that could cause a Disturbance in 15 minutes, or (3) affect situational awareness of the BES that would lead to a Disturbance required for real-time control of the BES. "What is real-time operations? To fully understand the definition of a BES Cyber System, the reader must pull out the NERC Glossary for the definition of Disturbance, BES, and ACE. Recommend an explicit definition that doesn't contain words from the NERC Glossary of Terms.NERC defines Disturbance as: 1. An unplanned event that produces an abnormal system condition. 2. Any perturbation to the electric system; or 3. The unexpected change to ACE (Area Control Error) that is caused by the sudden failure of generation or interruption of load.
41.b	CWLP Electric Transmission, Distribution and Operations Department	Disagree	It is unclear how the 15 minute time frame is to be construed for the purpose of defining a BES Cyber System. The 15 minute time frame appears arbitrary.

#	Organization	Yes or No	Question 1.b. Comment
42.b	FirstEnergy Corporation	Disagree	It is unclear if systems such as HP OpenView or a centralized logging system, which monitor alerts, are outside the scope of a BES Cyber System or if they are considered to affect situational awareness of a BES. As written, the definition could encourage entities to not install alerts so as not to have additional cyber systems. FE proposed change: "... or impact situational awareness that is deemed essential to the reliability of the BES". As an alternate, FE also supports EEI's suggested change to " ... materially disrupt situational awareness of the BES"The SDT should clarify how redundancy may impact the classification of BES Cyber Systems. For example, in a highly redundant architecture, there are many components whose loss would not impact or render essential systems as unavailable.The team should consider leveraging its work in developing the BES Cyber System and BES Cyber System Components to revise the existing Critical Cyber Asset.
43.b	Dairyland Power Cooperative	Disagree	It seems likely that a component could belong to multiple systems. How does this fit with the compliance regulations? Sentences are a little confusing with nested commas... It seems the intent is that 15 minutes applies to causing a disturbance, but it could be argued that it is ambiguous.
44.b	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
45.b	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested alternative definition: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
46.b	US Army Corps of Engineers, Omaha Distirc	Disagree	Need definitions of "restrict control and operation" and "affect situational awareness. These are very broad. If the intent of the standard is to create groups of cyber system

#	Organization	Yes or No	Question 1.b. Comment
			components and evaluate them based on their impact to system reliability why not state the definition in terms of the impacts. Suggest alternative wording - A Cyber System Component or logical grouping of Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, negatively impact one of the functions essential to the operation of the BES (Dynamic Response, Balancing Load and Generation, Controlling Frequency, Controlling Voltage, Managing Constraints, Monitoring & Control, Restoration of BES, Situational Awareness, Inter-Entity Real-Time Coordination and Communication, other functions as needed).
47.b	Garland Power and Light	Disagree	Need to add "scoping filter" as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states "typically excludes business, market function systems, and non real-time systems", then it is a good definition and we would agree.
48.b	The United Illuminating Co	Disagree	Not clear if the rendering unavailable, degraded, compromised or misused applies to the Cyber System or to the individual components of the Cyber System.Suggest: BES Cyber System - Comprised of One or more BES Cyber System Components. If a BES Cyber System when rendered unavailable, degraded, compromised, or misused could, within 15 minutes of such act, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.
49.b	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggested alternative definition:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness

#	Organization	Yes or No	Question 1.b. Comment
			of the BES. In addition, the phrase "situational awareness of the BES" needs some more clarity to derive determine what is intended.
50.b	Public Service Enterprise Group companies	Disagree	Please clarify that the 15 minute threshold means that if the cyber component would not cause a disturbance in the BES, or restrict control and operation, or affect situational awareness, within 15 minutes, the aggregation of BES Cyber System Components is not deemed to be a BES Cyber System and thus out of scope of Version 4.
51.b	Hydro One	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES for the support of real-time operations. The SDT should consider 30 minutes instead of 15 as this time is consistent with requirements of EOP-001 and IRO-001.
52.b	ISO New England Inc	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES for the support of real-time operations. - Recommend "30 minutes" to align with EOP standards - Please provide background for where the 15 minute recommendation came from.
53.b	Northeast Power Coordinating Council	Disagree	Recommend the following definition - A set of one or more programmable electronic device(s) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; and which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of

#	Organization	Yes or No	Question 1.b. Comment
			the BES for the support of real-time operations.
54.b	Con Edison of New York	Disagree	Regarding the BES Cyber System definition, specifically the qualification criteria “within 15 minutes could impact BES operation”, it is not clear how an entity will determine / distinguish which BES Cyber Systems could impact operation within 15 minutes versus which will not. This may be more challenging than distinguishing which Cyber Assets are essential to operation or not, as we do for version 2 of the CIPs. Our understanding is that the purpose of including the 15 minute period is to limit the application of CIP-010 to BES Cyber Systems impacting real time operations. An alternate way to address BES Cyber Systems impacting real time operations would be to look to the existing NERC Reliability Standards. The following definition language is recommended: “The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within the time period established in the applicable Reliability Standard(s), or if no time period exists, within 15 minutes of the BES Cyber System failure.”The following are examples of Reliability Standard citations: Standard BAL-005-0.1b - Automatic Generation Control R6. ... If a Balancing Authority is unable to calculate ACE for more than 30 minutes it shall notify its Reliability Coordinator. Standard EOP-001-0 - Emergency Operations Planning R2. The Transmission Operator shall have an emergency load reduction plan for all identified IROLs. ... The load reduction plan must be capable of being implemented within 30 minutes.
55.b	MWDSC	Disagree	Same general comments as for BES Cyber System Component. Also, "situational awareness" is redundant with the "monitoring and control" function as specified in Attachment 1 - see comment to Question 3 and suggested combination of terms. Disturbance reporting is required under EOP-004 - to avoid confusion or a conflict, definition needs a cross reference. Suggest changing last part of definition as follows:"... within 15 minutes, cause a Disturbance to the BES that requires a report pursuant to EOP-004, or affect the monitoring and control of the BES by a Transmission Operator,

#	Organization	Yes or No	Question 1.b. Comment
			Generator Operator, or Balancing Authority.
56.b	San Diego Gas and Electric Co.	Disagree	SDG&E is supportive of the "15 minute" criteria to help focus CIP-010 attention on real-time BES Cyber Systems. SDG&E recommends clarifying the categorization levels in conjunction with the 15 minute criteria, if the architecture or design includes the concept of redundant BES Systems (per Attachment I & II). Example: If a given BES System is potentially classified as a High BES System; but where an Entity has designed and operates a redundant BES System to enhance reliability of the BES Systems; and one which is in place to mitigate or reduce negative impacts to the BES, then the combined redundant system would not meet the criteria of a High BES System. Suggestions include incorporating a third classification category or filter which identifies potential High BES Systems which are treated separately, but have security controls applied.In the definition for a Component, the language states how a cyber system component "responds" to a BES condition or Disturbance or "enables" control and operation, but when talking about the System, a Component is spoken of in terms of a "causing" a disturbance, or "restricting" operation. Why is the piece of the whole (the component) "responding or enabling" yet when used in the context of "the whole" (the system) the piece is now labeled as "causing or restricting"? It is a bit confusing and redundant that a cyber system may also be a cyber system component. SDG&E is not certain what the value is with this level of granularity, and we are not certain that a "system component" definition is necessary. In addition, SDG&E suggests additional clarification on what "affect situational awareness of the BES" means.
57.b	Electricity Consumers Resource Council (ELCON)	Disagree	See comment on 1.a above.
58.b	Wolverine Power	Disagree	See comments listed for 1a
59.b	NextEra Energy Corporate Compliance	Disagree	See comments to 1.a. Furthermore, NextEra questions why there needs to be qualifiers like Disturbance. The industry understands which components need to be protected to safeguard Control Centers, Transmission and Generation. There would be a minimum

#	Organization	Yes or No	Question 1.b. Comment
			list developed that must be protected without qualifiers that could be misunderstood. In this regard, it is recommended that the following approach be adopted: BES Cyber System - A BES Cyber System Control Center, Transmission or Generation as defined in Section XX.
60.b	EEI	Disagree	See EEI's suggested wording in 1.a. Alternatively, EEI suggests: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
61.b	Tenaska	Disagree	Should only say: A grouping of one or more BES Cyber System Components. All other qualifiers should be in tables for Medium and High requirements. Careful consideration should be given to the "within 15 minutes" phrase, this time period may be too long or too short depending on the severity of the event, type of cyber asset, or the type of BES entity.
62.b	Madison Gas and Electric Company	Disagree	Suggest replacing the phrase, "cause a Disturbance on the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" with "cause an abnormal BES condition, degrade control and operation of the BES, or degrade situational awareness of the BES." The definition of Disturbance when used in this context is overly broad, for it includes "a perturbation to the electric system" or "the unexpected change in ACE that is caused by the sudden failure of generation or interruption of load." A perturbation to the electric system and a change is ACE are not qualified as to materiality. For example, a responsible entity's programmable device may be used in normal operation to curtail or interrupt relatively small amounts of load; such control of load (even simply for economic reasons) perturbs the electric system and affects ACE to some extent. Yet such effects are part of normal operation of the electric system. In addition, control and operation of the BES are always restricted to some extent; the concern is whether or not control and operation are degraded.

#	Organization	Yes or No	Question 1.b. Comment
			Likewise, the concern is whether or not situational awareness is degraded ("affect" could be in a way that is good or bad). New definition should read: One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause an abnormal BES condition, degrade control and operation of the BES, or degrade situational awareness of the BES.
63.b	ReliabilityFirst Staff	Disagree	Suggest thefollowing definition: "One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could impact realtime operation of the BES such as; cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES."
64.b	Allegheny Energy Supply	Disagree	Suggest: BES Cyber System - One or more BES Cyber System Components, performing one or more functions essential to the reliable operation of the BES, which if unable to perform its function, is misused, or operated by unauthorized personnel, could within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES that could lead to a BES Disturbance, or affect situational awareness of the BES that could lead to a BES disturbance.
65.b	Allegheny Power	Disagree	Suggested alternative definition: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or materially disrupt situational awareness of the BES.
66.b	SCE&G	Disagree	The 15 minute timeframe should be eliminated. There are too many variables in determining whether a system will have a 15-minute impact.
67.b	APPA Task Force	Disagree	The APPA Task force disagrees with the current definition for similar reasons stated above in regard to 1a. We offer the following simpler definition: “One or more BES Cyber System Components connected via routable protocol, which if rendered unavailable, degraded, compromised, or misused could cause an Adverse Reliability

#	Organization	Yes or No	Question 1.b. Comment
			Impact to the BES, or restrict control and operation of the BES for 30 minutes."See comments to Question 2 for time considerations. If the drafting team does not use this version we at least request that adding "connected via routable protocol" be included in some manner in the definition that is used.
68.b	US Bureau of Reclamation	Disagree	The identification of a BES cyber system based on the 15 minute criteria established here could be difficult to ascertain by those entities that do not directly operate or control the BES. Most entities can determine if it could compromize their respective BES assets. Further, this definition, if it does not establish additional qualifying criteria, would generally establish all Components identified under part 1.a., as Cyber Systems. As an example, an isolated single function cyber-based protective relay would qualify as a BES Cyber System Component under 1.a., but it would also qualify under criteria identified here in 1.b., since it is one or more "components" which could cause a disturbance if compromised - irrespective of the fact that it is not tied to any other components. Was this the intent of the drafting team?
69.b	LADWP	Disagree	The relative nature of the 15 minute criteria. What is the definition of a "Disturbance"?
70.b	Manitoba Hydro	Disagree	The term "misuse" in this definition is inappropriate. The definition misuse n. Improper, unlawful, or incorrect use; misapplication. 1. To use incorrectly. 2. To mistreat or abuse. The misuse of an asset describes the type of human action leading an effect on an asset, while the other terms unavailable, degraded or compromise describe more appropriately the state of the asset. The term misuse might lead into the area where analysis of one asset might cause an effect on another asset which is part of the BES Cyber System Component - secondary effects. Rather than using this approach the drafting team should list the types cyber assets which need consideration. i.e. support systems, HVAC, security, etc.) There may be Cyber system components linked to monitoring and/or network control that may operate periodically that could affect BES with disturbances. If there are any Cyber components that are not continuously or periodically (within 15 minute intervals) monitored for operational status that could either create or incorrectly not mitigate a network disturbance when they are

#	Organization	Yes or No	Question 1.b. Comment
			unavailable, they would not fit into the proposed definition. The definition needs clarification to include reference to all normal modes of operation of the BES Cyber System. For example, a protective relay has normal modes of operation of trip and restrain to trip. The 15 minute “real-time” criterion applies to both the trip and restrain to trip modes of operation. If a digital relay which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes of its trip mode or within 15 minutes of its restrain to trip mode (within 15 minutes of any normal mode of operation), cause or fail to mitigate a Disturbance to the BES, or restrict control and operation of the BES, it is a BES Cyber System.
71.b	American Electric Power	Disagree	The terms "situational awareness" is ambiguous; systems that are not needed for operating the BES, but provide information would be in scope. This definition appears to include items such as all meters, instruments, and transducers.
72.b	Seattle City Light	Disagree	The terms BES condition or Disturbance need to be further defined and clarified.
73.b	LCEC	Disagree	The time frame reference of "Within 15 minutes" could cause a great deal of confusion in identifying BES Cyber Systems. What is the basis for 15 minutes? How will the 15 minute test be audited?
74.b	Ameren	Disagree	The words “A Responsible Entity’s” should be added before the words “BES Cyber System Components” to make it clear that this only includes BES Cyber Systems components under the control of the Responsible Entity and specifically excludes entities such as Verizon. The last sentence the term Disturbance is too encompassing. Consider revising for more exact situations. The flow of the definition is difficult to read.
75.b	Matrikon Inc.	Disagree	This definition calls out those cyber systems that affect the BES in some way. During the application of CIP-010-1 there will be the need to classify and label those cyber systems that do not have any impact on the BES. That is the value of keeping the definition “Cyber Asset”, because it does not care about the relationship to BES

#	Organization	Yes or No	Question 1.b. Comment
			reliability, only to define the types of electronic systems to be evaluated as part of CIP-010-1 R1. My suggestion is to provide a label/definition for those systems that have no affect on BES, and allow "cyber assets" to remain.My second challenge when trying to apply this definition is how a "component" becomes a "system". The security controls of CIP-011 will be applied to individual cyber assets, and evaluating their individual impact on the BES is of ultimate importance. The need to apply the Impact requirements of CIP-011 appropriately will be satisfied when cyber assets share the same boundary access point, and all will have to inherit/conform to the same, and uppermost security controls criteria.In our CIP-002 definitions, we have defined a "system" as a group of cyber assets performing similar and/or cooperative activities in order to support a function. A similar definition can be used to support BES Cyber System, and the difference from BES Cyber System Component.
76.b	Duke Energy	Disagree	This definition is too broad. The phrase "compromised, or misused" could render compliance an impossibility, since administrators must have access to, and could misuse their access. Also, the phrase "situational awareness" should be clarified to include only that awareness required by System Operators to perform their reliability-related functions. Suggested clarifying change as follows: "One or more BES Cyber System Components which if rendered unavailable or degraded, could, within 15 minutes,: cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES required by System Operators to perform their reliability-related functions." Also, It is not clear if there will be any guidance around how 15 minutes threshold should be measured to ensure that numbers of interpretations for this threshold are limited.
77.b	Midwest ISO	Disagree	We agree that the time frame should be limited to the present but question the use of 15 minutes. Real-Time is a term that is included in the NERC Glossary. Why not use this term?
78.b	Pepco Holdings, Inc. -	Disagree	We appreciate the desire of the SDT to narrow BES Cyber Systems to real-time operations and understand the purpose of including 15 minutes to make that

#	Organization	Yes or No	Question 1.b. Comment
	Affiliates		distinction. We are not sure what the appropriate time frame would be and/or if 15 minutes is the correct time. So a Digital Fault Recorder which is traditionally used for after the fact analysis would not fall within the 15 minute window while and EMS/SCADA system which provides alarms and allows control of the BES would fall within the 15 minute window. Would a system that is compromised with a Trojan months or years ago but no action has been taken yet to compromise the BES meet the 15 minute window. Another possible approach is to list the real-time systems that need to be in-scope or considered.Because there does not seem to be a clear distinction between a BES Cyber System and a BES Cyber System Component, it would seem like a BES Cyber System could qualify as a BES Cyber System Component
79.b	Alliant Energy	Disagree	We believe the definition should be revised to: "One or more BES Cyber System Components which if rendered unavailable, degraded, or compromised could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES."
80.b	Independent Electricity System Operator	Disagree	We do not agree with the 15-minute qualifier. Any BES cyber system components that if tampered with can cause a disturbance to the BES or restrict control and operation of the BES, etc. should fall into this category since some components may have an impact on the BES if tampered with by more than 15 minutes before real time. To qualify the components to be only those that affect real time operation, we suggest wording such as "for the current hour and next hour operations" at the end of the sentence. Further, the term "misused" can be subject to a wide range of interpretation, and hence we suggest that it be replaced with "tampered with" or any term that the SDT thinks is more clear and appropriate.
81.b	We Energies	Disagree	We Energies agrees with the EEI Suggested alternative definition with minor modifications: BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes (15 minutes in this context is used to address real time operations and control of the BES), cause a Disturbance to the BES, or prevent control and operation of the BES, or

#	Organization	Yes or No	Question 1.b. Comment
			materially disrupt situational awareness of the BES.
82.b	MRO's NERC Standards Review Subcommittee	Disagree	We feel “affect situational awareness of the BES” should be removed, as this is already covered under “operation of the BES”. As written, situational awareness is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for operation of the BES. We also feel “misused” should be removed, as this is already covered under “compromised”.As currently worded, we also believe the intent of the 15 minute time frame is ambiguous. We would propose incorporating what we believe to be the drafting team’s true intent directly in to the definition, along with our other suggestions, as follows: One or more BES Cyber System Components which if rendered unavailable, degraded, or compromised could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES.
83.b	IRC Standards Review Committee	Disagree	We question the technical basis for a 15 minute time frame applied to any component that may cause a “Disturbance” to the BES. Without careful understanding of how the failure of the component could impact the BES 15 minutes may be too long or too short a time frame to allow recovery of the component or enable a mitigation solution. Further, we disagree that the disabling or degradation of any BES Cyber System Component would cause a “Disturbance” that is of significance to the integrity of the interconnected BES. To qualify the components to be only those that affect real-time operation reliability, we suggest wording such as “for the current hour and next hour operations” at the end of the sentence.The term “misused” can be subject to a wide range of interpretation, and hence we suggest that it be replaced with "tampered with" or any term that the SDT thinks is more clear and appropriate.
84.b	Southern Company	Disagree	We recommend the following definition: A system performing one or more BES functions identified in CIP-010 Attachment 1 and which if rendered unavailable, degraded, compromised, or misused would, within 15 minutes, adversely impact the real-time operational control of the BES.

#	Organization	Yes or No	Question 1.b. Comment
85.b	Covanta Energy	Disagree	Without a clear understanding of why '15 minutes' is the defined measure, it is difficult to support the definition.
86.b	Verizon Business	Agree	The “15 minute” criterion should be expanded in writing by the drafting team to provide a better sense of when the time starts. This could be done in an associated guideline or “Frequently Asked Question”

1.c. Control Center — A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to operation and restoration function, or
- Coordination of BES restoration activities.

Summary Consideration:

Many entities expressed concerns that the proposed definition of Control Center was too broad and could include various types of facilities not commonly considered control centers. Others questioned whether a Control Center should be defined as a collection of systems versus a physical facility housing such systems. Many entities indicated that the definition should be restricted to the functions of Reliability Coordinator, Balancing Authority, or Transmission Operator. Some expressed concerns about including situational awareness in the definition.

The SDT has modified the definition of Control Center to clarify that it is one or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more functions that support System Operators in the real-time operation of the BES. In consideration of the possible configurations where multiple locations may host such systems, the SDT used 'one or more' facilities. The SDT declined to limit the definition to of Control Center to facilities operated by RCs, BAs, or TOPs, since there are Control Centers operated by TOs and GOs/GOPs as well that must be protected.

The revised definition of **Control Center** is as follows:

One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:

- *Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,*

- *Inter-utility exchange of BES reliability or operability data,*
- *Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,*
- *Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,*
- *Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES*
- *Coordination of BES restoration activities.*

#	Organization	Yes or No	Question 1.c. Comment
1.c	BCTC		BCTC recommends the following aspects of this definition be revisited:Â Recommend the first bullet point be broken into three:ï,§ Supervisory Controlï,§ AGCï,§ Automatic Load SheddingÂ Recommend that the functions be categorized as “mandatory” for defining a facility as a control centre. These would include:ï,§ Supervisory controlï,§ BES and system status monitoringï,§ Alarm monitoringï,§ Coordination of BES restoration activitiesÂ To be considered a control centre the facility should have “two or more” of the functions listedÂ Remove “or” and replace with “and”Â For BES restoration a Utility may have workstations at an alternate site that by our everyday definition is not considered a control centre (i.e. alternate office building); how would these be classified within this definition? One of the questions we struggled with when looking as this definition was how to define a facility based on the number of RTUs present within them (i.e. one versus many) ... any advice?
2.c	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group		With no metrics defining anything upfront, it is possible to include applicability to very small entities. Control of two or more BES generation or Transmission Facilities with a combined historical demand of less than 500 MW should not be included in this definition. At some point, a defining line needs to be established to effectively define the bounds of the BES “castle” where defense of BES reliability is cost effective. Adding undue BES reliability compliance burdens on smaller DP/LSEs will ultimately add no BES reliability, and will hurt local distribution reliability efforts. If 500 MW is too large, then a conservative value can be agreed to and later revised as engineering studies become

#	Organization	Yes or No	Question 1.c. Comment
			available to justify a larger value.If that cell phone from 1.a. receives alarms from two or more locations and is used to make real time decisions it becomes a Control Center although it performs no control function and is not a center. Suggest that a Control Center be defined as a fixed server location.From the workshop, we realize that the lines separating the Component from the System and from the Center were intended to be flexible and up to the entity to consider system designs. The standard, however, does not read that way. We are concerned that based on the written standard the REs will not allow flexibility or even lines. All BES cyber devices, including every BES alarm displaying cell phone will be cast into all three buckets.
3.c	Dynegy Inc.	Agree with proposed definition	I agree but request additional detail examples be provided to determine specifically what these items are.
4.c	Southern California Edison Company	Agree with proposed definition	SCE requests clarification on systems and components that: (1) facilitate inter-utility exchange; and (2) devices that enable system status monitoring. Would devices such as email systems used for messaging and IP telephony systems in facilities be considered a “control center” or a BES Cyber System? The drafting team should issue guidelines on systems that directly perform BES reliability functions and systems/devices that are used by human operators for feedback prior to the manipulation of cyber components that directly impact the BES. It would also be beneficial for telecommunications equipment, which support a BES Critical Cyber system, be applicable only to COM-001 R2. If the intent of the drafting team is to limit the scope of cyber security controls to systems where real time BES impact is caused by direct human supervisory control over devices and systems, it should be clearly stated as such.
5.c	FEUS	Agree with proposed definition	What would it be considered if it only performed one function for a single BES facility at a single location? It would not be a control center.

#	Organization	Yes or No	Question 1.c. Comment
6.c	Minnesota Power	Agree with proposed definition	While Minnesota Power generally agrees with the proposed definition, it recommends that “(i.e., two or more)” be removed from the definition.
7.c	National Grid	Disagree with proposed definition	1. A control center is usually considered as a physical place with operators using various tools like EMS. The definition implies that a control center is a cyber asset. Isn't the Control Center much more than that? Maybe SDT is trying to define a "Control Center Cyber Asset". If so then SDT should use the term Control Center Cyber Asset. 2. National Grid seeks clarification on "Reliability" or Operability Data" since they can be subject to interpretation. 3. In bullet 3, the asset management piece should not be included. Also, if bullet 3 is indicating statuses like breaker status, then it is not required since it is covered in the preceding bullet. If not, then this should be better defined. 4. In bullet 4, there is no need to include "restoration function" as this is included in "operation" 5. In bullet 5, operators "coordinate" the BES restoration activities and not the cyber systems.
8.c	Progress Energy (non-Nuclear)	Disagree with proposed definition	1. From the definition, the ECC, DCC and the back-up control facilities would definitely be included. A substation that has a LAN connecting several cyber components would not be included. 2. Is a single generating facility the same as a single generating plant? Is a single generating plant a generating unit or a collection of generating units at 1 physical plant site? Clarify that a generating station control room is not a control center. 3. We need to be careful with definition of supervisory control as one possible interpretation of what the control room operator does is supervise the distributed control platforms that make up the plant control system. 4. These systems are independent only controlling one at a time. The key word here is “multiple”. Control rooms at some generation plants house multiple DCS systems. But, by design, each DCS controls its respective unit independently and are considered separate entities. I do not think this example would qualify as a Control Center. We can agree with this concept if they are talking about large regional control like the PJM interconnect or an ECC which it sounds like and NOT plant level Control Rooms. 5. A Control Center would operate

#	Organization	Yes or No	Question 1.c. Comment
			multiple generating Units with one control system.
9.c	Consultant	Disagree with proposed definition	1. The definition should identify that the "set of one or more BES Cyber Systems capable of performing..." are at a single location. If there are multiple locations where this capability exists then each location should be identified as a Control Center. 2. As stated, the definition creates a Control Center at every location where the capability "exists", whether this is a normal operation for each of those locations or is an emergency capability of each of those locations. If that is not the intent of the definition, then the distinction between normal and emergency (backup, off-normal) operations should be included in the definiton.
10.c	Progress Energy - Nuclear Generation	Disagree with proposed definition	A control center at a nuclear facility is different than this definition. I do not belive it is intended to apply to nuclear generation facilities, but rather the energy control centers that supervise bulk power loading functions.
11.c	Dairyland Power Cooperative	Disagree with proposed definition	A control center sound intuitively like a type of facility, but here is used as a term for a system(s) affecting multiple facilities. This will be confusing terminology.
12.c	Indeck Energy Services, Inc	Disagree with proposed definition	A control system that monitors through read-only access should not be categorized as a Control Center under CIP-010. A load aggregator is not identified as a potential Control Center.
13.c	Nuclear Energy Institute	Disagree with proposed definition	Agree with the exception that: The term “multiple locations” should be clarified to “multiple geographically distinct locations” to preclude confusion with a single facility with multiple generating units from being inappropriately identified as a control center.

#	Organization	Yes or No	Question 1.c. Comment
14.c	Alliant Energy	Disagree with proposed definition	Alliant Energy agrees with the EEI comments.
15.c	Pacific Gas & Electric Company	Disagree with proposed definition	Appears that under this definition of Control Center, several BES Cyber Systems or Components would be considered Control Centers such as:Distributed EMS or SCADA front-end processors Transfer Trip Protection Systems located at a specific substation control house that control other subs and/or generationSpecial Protection Schemes that control devices at multiple substations.Don't disagree on the importance of the items above to BES, just that defining them as a Control Center likely will lead to confusion.
16.c	City Utilities of Springfield, Missouri	Disagree with proposed definition	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
17.c	Ameren	Disagree with proposed definition	Clarify the definition to explain if it covers Power Plant control rooms, or if this is limited to transmission dispatching. Please clarify if “locations” refers to physical or electrical locations. Does “generation plants” refer to a Power Plant or generation “Facility” as defined by NERC; there use of plant vs. Facility is inconsistent. The definition appears to automatically cover all plant control rooms for any generator that see’s or controls the switchyard, is this the intent? In the third bullet, the term “and asset management” needs to be removed. As currently written, the inclusion of this term improperly suggests that facilities used for commercial and market purposes are covered by this definition.The definition of Control Center should only include those facilities where NERC certified operators are required for its operation.
18.c	CenterPoint Energy	Disagree with	Disagree - Control Center is a common industry term that often refers to a physical location. It should not be redefined under the CIP standards and should be deleted.

#	Organization	Yes or No	Question 1.c. Comment
		proposed definition	However, if the SDT feels a strong need to include this definition CenterPoint Energy suggest the following: A set of one multiple (i.e. two or more) BES Cyber Systems, located together at the same physical location, capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.
19.c	Tenaska	Disagree with proposed definition	Display and Inter-utility should be left out. Just display of will not hurt the reliability of the BES (PI data). Loss of inter-utility data need to have an N-11 type requirement with it. The loss of some percentage of data is tolerated in normal operation every day. The EMS/SCADA accounts for bad data. Consider using the definitions for Reliability Coordinator and Balancing Authority for clarity.
20.c	E.ON U.S.	Disagree with proposed definition	E.ON U.S. does not believe that the "display of BES reliability or operability data for the support of real-time operations" alone should qualify a locale as a control center. For example, view only information is often made available to plant operators Does "Alarm Monitoring" in the Control Center definition include sending alarms to remote ends of a transmission line from a substation? For example, carrier check-back and breaker failures. In addition how is transfer trip being addressed.?
21.c	Southern Company	Disagree with proposed	EOP-008, which is focused on control centers and control center functionality, does not contain or need a definition of the term. This implies that the CIP standards may not require a definition, either, and that any definition which is constructed must be done in light of the contents of EOP-008.If a definition is needed, we recommend the following

#	Organization	Yes or No	Question 1.c. Comment
		definition	definition:A location where one or more BES Cyber Systems are used to perform BA, RC, or TOP functions for generation Facilities or Transmission Facilities at multiple locations.If, for some reason, the existing definition must be modified, the following factors should be taken into consideration:Definition of Control Center - its our understanding that the Control Center definition is to be used to scope requirements based on 'environmental' factors and to differentiate it from generating plants and substations (field locations). So Control Center 'environment' is a 'data center' environment consisting of mostly traditional servers and workstations, Generation environment was a campus, plant type environment, and Transmission is an environment with unmanned field locations and mostly purpose built devices. These environments are then used to scope requirements appropriately based on the types of devices and the physical environment prevalent in that situation. The current definition of control center will pull in devices and systems from all the above environments and loses what we considered was the reason the environments were created and defined.For bullet 2...This clause pulls in far more facilities than are either intended or generally thought of as control centers. Things that would qualify: o An unattended remote data acquisition node o A standalone ICCP server feeding data to neighboring utilities o An RTU receiving data from multiple generating unitsThe definition should be modified to require multiple functions for a facility to qualify as a Control Center, and the second bullet, which includes many facilities which are not actually Control Centers and which does not add any additional facilities which should be considered as Control Centers, should be removed.In general, and in particular on bullet 4, processing is not a function of a control center; it's a function of the underlying cyber systems. The actual alarm monitoring, for example, is the key piece, and the wording about "processing" should be removed.For bullet 5...The fluid nature of disaster recovery makes this one worrisome. A makeshift command center set up in the wake of a natural disaster would qualify, even if all they had were laptops with no external network connection, creating some difficult access tracking issues. In general, the inclusion of BES restoration, if necessary, will need to be bounded carefully - one solution would be include the phrase "BES restoration specific to situational awareness".In addition, there are concerns about

#	Organization	Yes or No	Question 1.c. Comment
			small hydro units which can send control signals to other small hydro units being classified as control center locations.
22.c	Oncor Electric Delivery LLC	Disagree with proposed definition	Exclude “display” of data. Inclusion would allow an auditor to assess that the simple display of Responsive Reserve in an office constitutes a “control center”.
23.c	Southwestern Power Administration	Disagree with proposed definition	For the purpose of this standard it would be clearer if the definition would just identify what NERC functions are performed in the control center environment. This will also lessen the chance for confusion going forward with non-CIP reliability standards usage of the term “Control Center”. BES Control Center - A site where personnel can perform one or more of the following functions:Reliability CoordinatorBalancing AuthorityTransmission Operator
24.c	USACE HQ	Disagree with proposed definition	Given that Control Center is based on the definition of BES Cyber System Components and BES Cyber System, which I disagree with both, I must also disagree with this one.
25.c	Edison Mission Marketing and Trading	Disagree with proposed definition	I don't agree that status and alarm monitoring has anything to do with relaibility
26.c	San Diego Gas and Electric Co.	Disagree with proposed definition	If an asset to be evaluated for Control Center status is only one BES Cyber System, it does not seem to meet the definition of “a set”. Therefore, SDG&E suggests that the first sentence of the definition should be changed to read “One or more BES Cyber Systems capable of ...”Is a control center appropriately defined as one or more “BES Cyber Systems capable of performing...”, or would is it more appropriately defined as “A location where one or more BES Cyber Systems are monitored for proper performance

#	Organization	Yes or No	Question 1.c. Comment
			of one or more of the following functions (i.e., two or more)..."Why is control of two or more facilities required for this definition? How does a backup control center factor into this definition? In the past, the "two or more facilities" piece was part of the differentiation between a control room and a control center, but we don't see a definition of "control room" in this draft.
27.c	Dominion Resources Services, Inc.	Disagree with proposed definition	It is not clear whether the control center is the aggregate of the BES Cyber Systems or the physical space containing them. There is ambiguity as to whether the last phrase (at multiple...) belongs to the set of BES Cyber Systems or to the multiple facilities. Other definitions are of the form that "if it does this" then it is "this". It should be clarified that the presence of one or more of these functions does not make it a Control Center. For example, using a conference room or field office to direct BES restoration activities during an emergency does not make that conference room or field office a Control Center. The term should be limited to only those physical spaces used by a Balancing Authority, Reliability Coordinator and/or Transmission Operator in the performance of real-time functions, since these are the 3 entities charged with overall reliability functions for the BES. Dominion proposes the following definition of a Control Center: Control Center - The space where a Balancing Authority, Reliability Coordinator and/or Transmission Operator uses one or more BES Cyber Systems to perform one or more of the following functions for two or more geographically dispersed BES Generation or Transmission Facilities: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.

#	Organization	Yes or No	Question 1.c. Comment
28.c	Emerson Process Management	Disagree with proposed definition	It is very unclear how this term could be interpred for typical power generation plants. Very rarely, multiple generation facilities at different locations will be controlled under one physical control center. Control systems and control rooms are mostly located at the same place with the generation units.So, the term of Control Center in this standard may be totally inapplicable to BES generation facilities or entities.
29.c	Liberty Electric Power, LLC	Disagree with proposed definition	Many generation plants are not part of the current definition of BES. This standard is not the correct place to redefine BES, and any language which does so will force "No" votes on the standard, regardless of the merits of the rest of the document.
30.c	MidAmerican Energy Company	Disagree with proposed definition	MidAmerican Energy agrees with EEI's suggested modification to “Alarm monitoring” below:BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
31.c	Public Service Enterprise Group companies	Disagree with proposed definition	Mostly agree with the definition. However, the applicability of the first qualifier “(i.e., two or more)” is not clear. Does the qualifier apply to only “BES generation Facilities” or to “BES generation Facilities or Transmission Facilities”? Please clarify the language.
32.c	Regulatory Compliance	Disagree with proposed definition	Please clarify - for any control room at a generating facility that can remotely operate another site, whether or not it would be classified as a control center.
33.c	MWDSC	Disagree with proposed definition	Proposed definition conflicts with industry understanding and potentially with other standards. Attachment II assumes a Control Center is not just a collection of BES Cyber Systems gathering data, but rather a 24/7 facility staffed with certified power operators who take appropriate actions. Someone has to make decisions using the information being sent over cyber systems. Suggest changing definition as follows:"Control Center -

#	Organization	Yes or No	Question 1.c. Comment
			A facility staffed by a Transmission Operator, Generator Operator, or Balancing Authority who makes decisions based on information received from a set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations.
34.c	Con Edison of New York	Disagree with proposed definition	Regarding the definition of Control Center, as written, it appears that any facility can be deemed a Control Center. If a Transmission, Generation or other facility has a BES Cyber System that controls more than 1 generation or transmission facility it would be a Control Center. If so, this may be conflicting when addressing CIP-011-1 requirements that distinguish between Control Center and other facilities. This may also cause a transmission station that is connected to a generating station to be a Control Center if the station has an RTU cyber asset (with or maybe without an HMI) that can trip all station breakers (impacting the transmission station) and thereby trip the generator (impacting the generating station).
35.c	Wolverine Power	Disagree with proposed definition	See comments listed for 1.a
36.c	EEI	Disagree with proposed definition	See EEI's suggested wording in 1.a. Alternatively, EEI suggests:A modification to "Alarm monitoring":BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
37.c	WECC	Disagree with proposed definition	Seems to define the control center to try and exclude control rooms that only affect local facilities. Suggest rewriting to scope all bulleted functions performed inside a single location and EXCLUDING locations that only affect location facility operation.Based on the previously defined term "BES Cyber Systems" it is redundant to characterize a Control Center as a "set of one or more."The following rewrite is

#	Organization	Yes or No	Question 1.c. Comment
			proposed;Control Center - A facility used to implement a BES Cyber System(s) to perform one or more of the following functions for BES Generation Facilities, BES Transmission Facilities, and/or Distribution Facilities located at two or more locations: o Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems, o Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations, o BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES), o Alarm monitoring and processing specific to operation and restoration function, or o Coordination of BES restoration activities.Distribution is included in this suggested rewrite based on its inclusion in the Applicability List as “Distribution Provider.”
38.c	Madison Gas and Electric Company	Disagree with proposed definition	Suggest removing the comma after "Transmission Facilities." With the comma, the subsequent phrase, "at multiple (i.e., two or more) locations," could be interpreted to apply to "one or more BES Cyber Systems" rather than BES Generation or Transmission Facilities.The term "location" is ambiguous in the context of the definition. For example, multiple generators at the same generating plant are placed in multiple locations (unless they impossibly occupy the same physical space). The intent of the qualification "at multiple locations" seems to be to exclude generating plant control systems, yet the definition could be read to potentially include generating plant control systems as Control Centers. Recommend modifying the definition to provide more specificity.Similar to the definition of BES Cyber System, the definition of Control Center does not provide criteria for aggregating BES Cyber Systems to define the "set of one or more BES Cyber Systems" that comprise a Control Center.New definition should read:Control Center - A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

#	Organization	Yes or No	Question 1.c. Comment
39.c	Entergy	Disagree with proposed definition	Suggest: A) Changing definition to speak specifically to "Functions" in Attachment I; and delete "for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations." B) Delete all bullets and rely on list of Functions as sole qualifiers. C) Note: close scrutiny of this definition is needed relative to EOP-008 (Project 2006-04: Backup Facilities; nearing final ballot) to avoid conclusion.
40.c	Green Country Energy	Disagree with proposed definition	Suggested definition:Control Center - A set of one or more BES Cyber Systems capable of performing one or more of the following functions at two or more BES generation Facilities, or Transmission Facilities at two or more locations:
41.c	Allegheny Power	Disagree with proposed definition	Suggested modification to "Alarm monitoring" o BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
42.c	Allegheny Energy Supply	Disagree with proposed definition	Suggested modification to "Alarm monitoring"- BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or
43.c	Constellation Power Source Generation	Disagree with proposed definition	The "Acquisition, aggregation, processing..." function that a Generation Management System (GMS) or a marketing system would fall under scope of a "control center" though it would make more sense (in reliability terms) for it to be just a BES cyber system. A clarifying statement is needed to exclude marketing and GMS systems from this control center definition. The definition of control center is too broad in only requiring performance of one of the functions to meet the definition. A control center is commonly understood to be a location, not a system, where at least 4 of the 5 functions are performed, if not all 5 functions. This definition eliminated the concept of a control center as a defined space with operating systems and instead identifies a control center

#	Organization	Yes or No	Question 1.c. Comment
			as cyber systems which pull in work spaces that should not be in scope.
44.c	APPA Task Force	Disagree with proposed definition	The APPA Task force is concerned that under the proposed definition, a substation control room could be considered a "Control Center." Therefore, we offer the following clarification for your consideration:"A set of one or more BES Cyber Systems at centralized, primary or back-up locations that enable centralized operation of a Reliability Coordinator, Balancing Authority or Transmission Operator."
45.c	Xcel Energy	Disagree with proposed definition	The definition needs to clarify that it applies to interconnected control systems. For example, two independent control systems with no interdependency that operate generation units at separate locations should not be defined as a control center.
46.c	Constellation Energy Control and Dispatch, LLC	Disagree with proposed definition	The definition of Control Center is too broad in only requiring performance of one of the functions to meet the definition. A Control Center is commonly understood to be a location not a system, where at least four of the five functions are performed, if not all. This definition eliminates the concept of a control center as a defined space with operating systems and instead identifies a control center as systems which would pull in work spaces that should not be considered Control Centers. Remove AGC Systems from function 1. Automatic Generation Control is defined to be Equipment (not a system) that automatically adjusts generation in a Balancing Authority from a central location to maintain the BAs interchange schedule plus Frequency Bias. The Equipment that automatically adjust generation is located at the generation site not in the Control Center. The Control Center EMS has the ability to send a signal to a generator, but not to automatically adjust the generation. Rather the generator is set up to pick up the signal in a central control system at the site and use the signal to change its operating level with in established operating parameters in accordance with established capability. The definition of Control Center should focus on the systems in a Control Center that can actually automatically operate equipment, i.e. Supervisory control of BES assets at generating plants, transmission facilities and substations is a sufficient description of these type of Control Center functions.Remove asset management from function 3.

#	Organization	Yes or No	Question 1.c. Comment
			Unless this term is defined to narrow the scope as related to Control Center functions, this term is loosely used in the industry and would result in too broad of an application of this function.It may be worth including a data acquisition timing reference to appropriately narrow the scope as well. Control Centers are processing data in terms of cycles or seconds and many of the function described may be performed by systems using longer intervals and these longer interval systems should not be pulled into the definition.
47.c	Constellation Energy Commodities Group Inc.	Disagree with proposed definition	The definition of... "capable of performing one or more..." should be changed to "capable of performing four or more..."The definition of Control Center is too broad in only requiring performance of one of the functions to meet the definition. A Control Center is commonly understood to be a location not a system, where at least four of the five functions are performed, if not all. This definition eliminates the concept of a control center as a defined space with operating systems and instead identifies a control center as systems, which would pull in work spaces that should not be considered Control Centers. Remove AGC Systems from function 1. Automatic Generation Control is defined to be Equipment (not a system) that automatically adjusts generation in a Balancing Authority from a central location to maintain the BAs interchange schedule plus Frequency Bias. The Equipment that automatically adjusts generation is located at the generation site not in the Control Center. The Control Center EMS has the ability to send a signal to a generator, but not to automatically adjust the generation. Rather the generator is set up to pick up the signal in a central control system at the site and use the signal to change its operating level within established operating parameters in accordance with established capability. The definition of Control Center should focus on the systems in a Control Center that can actually automatically operate equipment, i.e. Supervisory control of BES assets at generating plants, transmission facilities and substations is a sufficient description of these types of Control Center functions.Remove asset management from function 3. Unless this term is defined to narrow the scope as related to Control Center functions, this term is loosely used in the industry and would result in too broad of an application of this function.It may be worth including a data acquisition timing reference to appropriately narrow the scope as well. Control Centers

#	Organization	Yes or No	Question 1.c. Comment
			are processing data in terms of cycles or seconds and many of the function described may be performed by systems using longer intervals and these longer interval systems should not be pulled into the definition.Typically, BES restoration processes are coordinated with manual processes, and are not Cyber System related.
48.c	Platte River Power Authority	Disagree with proposed definition	The function"BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES)," doesn't clearly represent the real-time nature of the function. "System" is already included in BES. Suggested revision:BES real-time status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
49.c	CWLP Electric Transmission, Distribution and Operations Department	Disagree with proposed definition	The last two bullet points should be removed. The first is redundant and the last muddies the concept of control center. Restoration activities could be coordinated from a bucket truck or a temporary command center. These functions are actually human interactions not cyber systems.
50.c	US Bureau of Reclamation	Disagree with proposed definition	The term "BES asset" is not defined. The requirement should either propose a definition or the language in the requirement should be modified to refer to "BES Facilities" both of which are defined in the NERC Glossary of Terms.
51.c	LCEC	Disagree with proposed definition	The term "locations" needs to be defined. Should the human/machine interface be considered in defining a control center? Ensure that control rooms are not considered as control centers per this definition.
52.c	Southwest Power Pool Regional Entity	Disagree with	The use of "multiple (i.e., two or more)" twice in the same sentence is confusing. Consider changing the definition to read "A set of one or more BES Cyber Systems

#	Organization	Yes or No	Question 1.c. Comment
		proposed definition	capable of performing one or more of the following functions for multiple (i.e., two or more) geographically disperse BES generation Facilities or Transmission Facilities:"
53.c	Hydro One	Disagree with proposed definition	There is a gap regarding centralized configuration of BES Cyber Systems. The current definition of control center does not include a centralized system used for maintaining or configuring remote equipment such as RTUs or relays.Based on the control centre proposed definition all hub sites would be deemed within the definition of control centers. We would like the clarification if the auxiliary systems (High pressure air systems, cable temperature monitoring, QFW sag monitoring, DC inverters, PLCs, substations WANs, teleprotections, synchrophasors etc.) would be considered as BES Cyber System Components. As proposed, this definition would have massive implications to Hydro One in terms of implementation, capital cost, OM&A expenses etc.
54.c	Northeast Power Coordinating Council	Disagree with proposed definition	There is a gap regarding centralized configuration of BES Cyber Systems. The current definition of control center does not include a centralized system used for maintaining or configuring remote equipment such as RTUs or relays.
55.c	Bonneville Power Administration	Disagree with proposed definition	Third bullet should make it more clear that only real-time management (control and operation) is relevant. The example is for real time control; changing "e.g." to "i.e" would be sufficient. In addition, the way the definition is written it is possible that a substation could end up being identified as a Control Center. The definition needs to be clear that these are facilities whose prime purpose is to be control centers, not just substations that happen to have information covering other substations, or even possibly the ability to exercise some control over another substation.
56.c	Exelon Corporation	Disagree with proposed	This definition does not align with the commonly understood definition of control center and could be interpreted to apply to multiple unmanned locations housing servers.

#	Organization	Yes or No	Question 1.c. Comment
		definition	
57.c	NextEra Energy Corporate Compliance	Disagree with proposed definition	This definition needs to be more specific. NextEra suggest removing "capable" in the first line and removing or better defining "coordination" and "restore BES activities." NextEra also recommends defining control center as having the "Primary function."NextEra also suggests being clear on whether remote Control Centers are included, and, if so, CIP-011 needs to be very clear on any differences in the protection of remote control centers versus primary control centers. NextEra will be providing additional comments in the future.
58.c	Reliability & Compliance Group	Disagree with proposed definition	This definition seems to include control room as a Control Center. Does this mean a control room can be considered as a control center? Normally a Control Center requires having real time operation functions. The way it is stated above if you meet one of the last two functions, it is qualifies as a control center
59.c	Duke Energy	Disagree with proposed definition	This definition should be revised to clarify that a Control Center only includes facilities required to be staffed by NERC-certified operators. The revised definition should explicitly clarify that the term Control Center does not include the control room for a multiple generating unit site. Also, the use of the capitalized term "Facilities" continually causes confusion during audits, because, as the term is defined, even a single generating unit site could contain multiple "Facilities" (e.g. a line, a generator, a shunt compensator, transformer, etc.)Also, the phrase "capable of" is open to interpretation, and should be replaced with the phrase "operationally responsible for". Also, the phrase "for the support of" in the second bullet is open to interpretation, and should be replaced with the phrase "essential to".
60.c	Old Dominion Electric Cooperative	Disagree with proposed definition	This seems to widen the definition of control center to the point of being overreaching.

#	Organization	Yes or No	Question 1.c. Comment
61.c	Pepco Holdings, Inc. - Affiliates	Disagree with proposed definition	We agree with EEI's comments. Do transmission facilities include substations or does it reference just the transmission line components?
62.c	FirstEnergy Corporation	Disagree with proposed definition	We are unclear why 'control center' is being redefined as a logical set of cyber systems rather than a physical site which accommodates the functions traditionally identified with control centers. This definition appears to align with legacy architectures, where the control center serves as a communications hub and data center, thus creating a single point of failure. Modern architectures that employ best practices for reliability, redundancy, and diversity do not employ that structure. Since this is a significant departure from the commonly understood definition of 'control center', it is unclear how this definition will impact compliance to the newly proposed standards.
63.c	GTC & GSOC	Disagree with proposed definition	We do not agree with this definition. We believe that it will capture a large number of systems that are not part of what is commonly understood to be a control center. For example, an RTU acting as a data concentrator acquires data from multiple locations and supports real-time operations, but is not itself a control center. In addition, the term "BES assets" is an artifact of the version 1, 2, and 3 CIP standards and should either be replaced or clarified. More basically, though, we question the need for this definition. Its primary function appears to be as a scoping criterion for CIP-011 in the same manner that generation [sic] Facility and Transmission Facility are. However, the SDT did not feel the need to define either of those terms. We recommend that this definition may be better suited for a guidance document.
64.c	We Energies	Disagree with proposed definition	We Energies agrees with EEI Suggested modification to "Alarm monitoring" with minor modifications: o BES Alarm monitoring and processing specific to BES real-time operation or BES restoration function, or Suggested modification to "Acquisition" bullet o Acquisition, aggregation, processing, inter-utility exchange or display of BES reliability or operability data for the support of real-time BES operations.

#	Organization	Yes or No	Question 1.c. Comment
65.c	Independent Electricity System Operator	Disagree with proposed definition	We generally agree with the description in the definition, but do not agree with the term “control centre” as it confuses with the traditional control centre of BES operations. We suggest the term be changed, for example, to “BES Cyber Cluster”, or “BES Cyber Control Cluster”.
66.c	IRC Standards Review Committee	Disagree with proposed definition	We generally agree with the description in the definition, but do not agree with the term “control centre” as it confuses with the traditional control centre of BES operations. We suggest the term be changed, for example, to “BES Cyber Cluster”, or “BES Cyber Control Cluster” or “BES Control System”.
67.c	Midwest ISO	Disagree with proposed definition	What is really being described is a control system and not a control center. A control center implies physical attributes that are not described in this definition. We suggest to modify the definition to control system rather than control center.
68.c	Florida Municipal Power Agency	Disagree with proposed definition	With this definition, a substation control room can be a “Control Center”. A Control Center has other characteristics associated with it that make it a control center, i.e., “centralized operation”, the reverse of the term. FMPA suggests a simpler definition:”A set of one or more BES Cyber Systems at centralized, primary or back-up locations that enable centralized operation of a Reliability Coordinator, Balancing Authority or Transmission Operator.”

2. **The definition of BES Cyber System limits the scope of the definition and the applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems with an operational time horizon of 15 minutes. Do you agree with this scope of applicability? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

While there was general agreement with scoping the applicability of the standards to "real-time" systems, many entities questioned the source of 15 minutes as the scoping time. Some commenters expressed concerns about the auditability of this qualification in defining the scope of applicability.

In selecting the 15-minutewindow, the SDT reviewed various reliability standards and identified two widely used time horizons: 30 minutes and 15 minutes. The intent of the SDT is to include those systems that impact "real-time" operation of the BES. The SDT used a 15-minute window to qualify the "real-time" nature of the impact and felt that a 30-minute window would include those systems that might not be considered as "real-time".

The proposed definition of a **BES Cyber System** has been revised as follows:

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

#	Organization	Yes or No	Question 2 Comment
2.1	USACE HQ		I disagree with the scope and disagree with expanding the scope. The use of a time limit to represent real-time should not be present given that is lacking documentation support for the number. Either introduce a definition for real time for CIP purposes or provide support for the risk-informed dentition of using 15 minutes as the limit
2.2	Arizona Public Service Company		The 15-minute criteria specified as part of the definition of a BES Cyber System may both lead to confusion and/or act as a loophole to exclude BES Cyber System Components from further consideration. Confusion may be caused by likely differing interpretations of "restrict control and operation of the BES, or affect situational awareness of the BES". Without more specific definitions, each Entity may utilize different criteria for determining whether control and operation has been 'restricted' or whether situational awareness has been 'affected'. Such potential ambiguity may also allow Entities to utilize

#	Organization	Yes or No	Question 2 Comment
			excess discretion in this determination in order to 'exclude' Cyber System Components from categorization. A suggestion would be to attempt to avoid such vague terms if a timeline is specified in the definition at all, or to avoid a timeline in the definition and add time windows to the Impact Categorizations. Examples of terminology changes include using the term 'impede' rather than 'restrict' (as some restriction may be tolerable, but impede strengthens the concept being conveyed) or using the phrase 'impact operational decision making' rather than 'affect situational awareness' (as such a phrase might be less likely to be misinterpreted outside of Power Operations expertise).
2.3	Nuclear Energy Institute	Agree with scope	A recommended change to BES Cyber System Component has been proposed to clarify that the intent is to protect real-time operations. NEI recommends examples of systems that would fall in and outside this scope.
2.4	US Army Corps of Engineers, Omaha Distirc	Agree with scope	Agree with limiting scope to real-time systems with an operational time horizon of 15 minutes. However the wording of the definition needs to be strengthened because the intended meaning of the definition as "real-time" systems with an operational time horizon of 15 minutes" was not clear until.
2.5	Entergy	Agree with scope	Agree with scope limitation to "real-time operations." Suggest: Rule 706 be carefully reviewed to assure this is not countervailing to FERC directives; their directives suggest a broader scope of applicability.
2.6	Allegheny Power	Agree with scope	Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.7	EEI	Agree with	Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be

#	Organization	Yes or No	Question 2 Comment
		scope	appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.8	MWDSC	Agree with scope	Also need to identify who makes the real-time operational decisions, i.e., Transmission or Generator Operator or Balancing Authority. See suggested changes in comments to question 1.b.
2.9	City Utilities of Springfield, Missouri	Agree with scope	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
2.10	Dominion Resources Services, Inc.	Agree with scope	Dominion supports the inclusion of "within 15 minutes". It is important to establish a reasonable boundary condition for the real-time or near real-time effects of the BES Cyber System and 15 minutes provides adequate time for the effects to be mitigated to prevent further harm to the BES.
2.11	Southwest Power Pool Regional Entity	Agree with scope	Entities today eliminate assets from the Critical Asset list because they assume a mitigation to a voltage instability or thermal overload is available and will always be successful. Consider modifying the definition to read "...could, if not mitigated within 15 minutes,..."
2.12	Southwestern Power Administration	Agree with scope	Fifteen minutes seems to be a reasonable operational horizon, but should the language be modified in such a way to allow for an operational time horizon of approximately 15 minutes in order to discourage "clock watching" by entities and/or auditors to reach a conclusion of either fourteen or sixteen minutes.
2.13	Platte River Power Authority	Agree with scope	I agree so long as the BES Cyber System definition is updated to more clearly explain the horizon. For example:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within an

#	Organization	Yes or No	Question 2 Comment
			operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.
2.14	MidAmerican Energy Company	Agree with scope	MidAmerican Energy agrees with EEI's affirmation below:Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.15	Progress Energy (non-Nuclear)	Agree with scope	See comment for question 1b.
2.16	APPA Task Force	Agree with scope	The APPA Task force agrees with the proposed definition, but offers the following suggestions:It seems that the 15 minute horizon is arbitrary. We suggest aligning the time to an already determined time limit in the standards. For instance, TOP-004-2, R4 allows 30 minutes for a Transmission Operator to restore the system to a known operating state within operational limits from an “unknown operating state”, which seems to be a good metric to use since loss of situational awareness at a Control Center results in an “unknown operating state”, which seems to correspond with the longest time frame of Attachment I to CIP-010. We understand that other commenters are submitting alternative language. We can support alternative options if they are based on existing NERC defined terms or already determined time limits.
2.17	Bonneville Power Administration	Agree with scope	The definition clearly ties the scope of the standard to real-time control. The time limit clearly separates real-time from long-term. The choice of 15 minutes versus some other duration is not as important as limiting the duration.While we agree with the scope, we don't believe the definition of BES Cyber System makes it clear that the scope is limited to real-time operation systems. The definition of BES Cyber System doesn't include the words real-time. For CIP-002, BPA identifies only control center systems used for real-

#	Organization	Yes or No	Question 2 Comment
			time controls as Critical Cyber Assets. This scope is consistent with what BPA does now for control center cyber systems.
2.18	Southern California Edison Company	Agree with scope	The drafting team should provide justification on the use of a 15 minute window for a BES cyber system to cause a Disturbance. Is the drafting team suggesting registered entities simulate disturbance events in 15 minute increments as a criterion in engineering studies to assess device capability that may be the justification for an impact based assessment methodology? If so, the drafting team needs to clarify this.SCE suggests removal of the 15 minute qualifier if no clear operational justification exists for the choice of such timeframe. While a three year timeframe for engineering studies is an acceptable, the constraints necessary for inclusion within the study, to look for specific disturbance conditions, may be difficult to implement.
2.19	Midwest ISO	Agree with scope	We agree in general. However, we do not necessarily agree with 15 minutes. Please see our response to Question 1.b.
2.20	Pepco Holdings, Inc. - Affiliates	Agree with scope	We agree with EEI's comments regarding the intended scope (i.e. limit to systems that impact the real-time real-time operations of the BES) and suggestions. Please also reference response to 1b.
2.21	We Energies	Agree with scope	We Energies agrees with EEI comments. Agree with the intended scope. It is appropriate to focus and prioritize the establishment of security controls to address real-time operations of the BES. It may be appropriate to add language explaining why certain items are in or out of scope. For example, computers that are used to perform long term system modeling and engineering design should not be subject to the same security requirements as real-time systems.
2.22	GTC & GSOC	Agree with scope	We understand the intent of the 15 minute aspect of the defined scope, but believe it will be difficult to implement and audit. Otherwise, we recommend the revised definition in 1b

#	Organization	Yes or No	Question 2 Comment
2.23	Duke Energy	Agree with scope	With the clarifications we've made above, we agree with the scope of applicability.
2.24	ISO New England Inc	Disagree with scope	- Recommend "30 minutes" to align with EOP standards- Please provide background for where the 15 minute recommendation came from
2.25	ReliabilityFirst Staff	Disagree with scope	Assuming the 15 minutes identified here is the same 15 minutes used in question 1.b above, we believe the scope should be 5 minutes.
2.26	Tenaska	Disagree with scope	Careful consideration should be given to the "within 15 minutes" phrase, this time period may be too long or too short depending on the severity of the event, type of cyber asset, or the type of BES entity. The Operational Time Horizon should be based on the potential severity of the event as well as the availability of other systems that can provide the same functionality.
2.27	Cogeneration Association of California and Energy Producers & Users Coalition	Disagree with scope	Comments to Questions 1.a and 1.b apply here also.
2.28	ERCOT ISO	Disagree with scope	Comments: The 15 minute requirement does not align to the other reliability standards. Recommend changing to 30 minutes to align with the EOP standards.
2.29	CenterPoint Energy	Disagree with scope	Disagree - CenterPoint Energy is concerned with the definition as stated above in response to 1.b. In addition, the SDT has offered no basis for the 15 minute time horizon.

#	Organization	Yes or No	Question 2 Comment
2.30	E.ON U.S.	Disagree with scope	E.ON U.S. seeks clarification of whether the 15 minutes captures the intent of the 'Restoration of BES" function identified in Attachment 1 of CIP-010
2.31	Exelon Corporation	Disagree with scope	Exelon suggests that the time period should not be stated in specific minutes. The standard should be revised to "One or more BES..., or misused could, without sufficient time to take mitigating action, cause a disturbance to the BES,..." The 15 minute timeframe is inconsistent with other standard language. Specifically, TOP-004-2 R.4. has a 30 minute response requirement.
2.32	LCEC	Disagree with scope	I am concerned that a time based definition will lead to confusion and create a difficult situation from an audit perspective. I agree that the standard should exclude "situational awareness" related functions that are not real-time in nature and do not provide the primary operational monitoring or control function of the BES.
2.33	Matrikon Inc.	Disagree with scope	I am trying to determine where to insert this operational time horizon into the evaluation criteria. Due to the room for interpretation, I don't yet support or reject the use of 15-minutes, or an appropriate duration. Fundamentally, there is no clear definition or instruction on how this can be used as criteria for determining Impact Level of cyber systems.I worry there is room for different interpretations, putting an entity trying to comply with the new CIP-01x standard at a competitive disadvantage to another entity that takes a different approach. I foresee 2-3 places where the time horizon could be inserted into a Responsible Entity's interpretation of BES Cyber Systems, I am hoping a tighter definition will address this issue.First Interpretation Scenario:1. The entity first determines the Impact Rating of each individual Cyber System using Attachment 2.2. Do they now evaluate the impact rating against the time horizon? Let us assume the Cyber System has High Impact. But if there is no effect in 15 minutes, does that mean: 2a. I automatically assign a Medium impact Rating? 2b. Or, I now evaluate it against the Medium impact criteria?3. If it continues to have no impact in 15 minutes to the Medium criteria, then is it a Low Impact BES Cyber System?Second

#	Organization	Yes or No	Question 2 Comment
			Interpretation Scenario:1. The entity first determines the Impact Rating of each individual Cyber System using Attachment 2. 1a. Let's now assume that the rating of High/Medium/Low is assigned to each BES Cyber Component and cannot be changed.2. Do they now go through the complete list of Cyber Systems looking for those which could affect any reliability function within 15 minutes? 2a. This may bring in other support systems like HVAC, UPS, CEMS opacity readings for generation, water supply and others that are not explicitly named in Attachment 1.Third Interpretation Scenario:1. An event has occurred at the facility that some action needs to be taken. There is the capability to notify the authority, and shutdown/bypass safely within 5-10 minutes.2. If the Responsibility Entity has the ability to exceed 15-minutes before taking action, then is this no longer an impact to the BES, and subsequently falls to the bottom and become Low Impact. 2a. For example, coal handling is down but we have some coal left on the conveyor, and the boiler is still hot so we have time to respond. 2b. For example, water supply is dropping but do not have to take action within 15 minutes. 2c. For example, vibration or emissions data is high, but we don't have to take action, within 15 minutes.Please provide additional information and guidance on how the 15-minute time horizon is to be applied to systems.
2.34	CWLP Electric Transmission, Distribution and Operations Department	Disagree with scope	It is unclear how the 15 minute time frame is to be applied.
2.35	Emerson Process Management	Disagree with scope	It really depends on how we view this issue. If I understand this intent correctly, the current language is trying to state that the BES reliability will be suffered if the BES cyber system is unavailable for more than 15 minutes. In another word, if the BES cyber system is failed for more than 15 minutes and the BES is not suffered, this system will be not categorized as BES Cyber System. This definition is very difficult in interpretation for power generation. If a plant has a 2000MW generation capacity and its water treatment cyber system is failed, the plant itself can sustain for a while, but not too long. After this grace period, the unit(s) will be shut down. The 2000MW will be lost. Does this affect

#	Organization	Yes or No	Question 2 Comment
			BES reliability? This is the confusion.
2.36	Florida Municipal Power Agency	Disagree with scope	It seems that the 15 minutes is arbitrary. FMPA suggests aligning the time to an already determined time limit in the standards. For instance, TOP 004 2, R4 allows 30 minutes for a Transmission Operator to restore the system to a known operating state within operational limits from an "unknown operating state", which seems to be a good metric to use since loss of situational awareness at a Control Center results in an "unknown operating state", which seems to correspond with the longest time frame of Attachment I to CIP-010.
2.37	Seattle City Light	Disagree with scope	It will be difficult to quantify the impact of systems within a window of time - this would be a qualitative assessment which invites a tremendous amount of subjectivity.
2.38	Garland Power and Light	Disagree with scope	Need to add "scoping filter" as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states "typically excludes business, market function systems, and non real-time systems", then it is a good scope and we would agree
2.39	Kansas City Power & Light	Disagree with scope	No. Including "within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES" in the definition provides a difficult set of parameters that encourages issues with interpretation of what would constitute the situations under which "within 15 minutes" applies, as well as, what constitutes "restricted control or generation"? It is understood the Drafting Team is trying to capture the essence of those systems that have a real-time impact on the BES, however, it is recommended to limit the scope of the applicable "BES Cyber

#	Organization	Yes or No	Question 2 Comment
			System" to those systems that support facilities that are identified as critical to the reliability of the transmission grid determined by regional system study.
2.40	Covanta Energy	Disagree with scope	Not clear as to why 15 minutes is the optimal number... would like more basis information prior to supporting.
2.41	IRC Standards Review Committee	Disagree with scope	Please see our comments under Q1b
2.42	Independent Electricity System Operator	Disagree with scope	Please see our comments under Q1b.
2.43	Public Service Enterprise Group companies	Disagree with scope	PSEG agrees that cyber protections should be mandated only for real-time operations systems.
2.44	National Grid	Disagree with scope	Real time operation of the system typically implies SCADA. If protection systems are part of the real time operations then as stated in 1b, the 15 minute time horizon may not be adequate. 15 minute time limitation also does not appear realistic. The vulnerability can exist beyond this timeline and can be equally catastrophic.
2.45	Electricity Consumers Resource Council (ELCON)	Disagree with scope	See comment on 1.a above.
2.46	NextEra Energy Corporate Compliance	Disagree with scope	See comments to 1a. NextEra believes if this approach is maintained despite these concerns, then this section needs clarity regarding 15 minute time horizon regarding recoverability. As written, the definition encompasses and overlaps normal operations

#	Organization	Yes or No	Question 2 Comment
			systems and recovery timeframes and does not address impacts to the BES beyond normal reliability operations.
2.47	Manitoba Hydro	Disagree with scope	See comments to Question 1.6
2.48	BCTC	Disagree with scope	See previous response
2.49	Network & Security Technologies Inc	Disagree with scope	See response to 1.b., previous
2.50	Puget Sound Energy	Disagree with scope	See response to question 1b. While it seems realistic, it is unclear how to prove something is within the 15 minute timeframe or not and unclear how this could be tested during an audit that something should have been included or not included. Some examples would be beneficial. Also PSE agrees with the scope of the definition, but is concerned with the vagueness of two of the terms used in the definition: “restrict” and “affect”. PSE agrees with the definitive language of “cause a Disturbance”, as that is a measurable level of compliance. The current standard has too many vague terms that are left open for interpretation.
2.51	WECC	Disagree with scope	Suggest SDT re-evaluate if reliability coordination systems such as Coordinated Outages, Historian, or Next Day Studies should be excluded from scope of these standards.Also, see response to 1c
2.52	Indeck Energy Services, Inc	Disagree with scope	The 15 minute time horizon needs to exclude events that the BES normally resolves within 15 minutes. Many events could take place in significantly less time. Normal operations work within the 10 minute horizon for measurements such as controlling

#	Organization	Yes or No	Question 2 Comment
			ACE. Not everything that happens within 15 minutes necessarily affects BES ALR. A single 15 minute time horizon appears to cast the net too widely. The time horizon needs to be specified for each of the Functions in Attachment I.
2.53	FirstEnergy Corporation	Disagree with scope	The 15 minute time limit causes confusion on how the definition will be applied in practice, since in most cases the loss of a component creates a probabilistic risk and not a certain risk.FE suggest that the SDT avoid the use of the 15 minute reference and consider incorporating the existing NERC glossary terms of "Real-time" and "Real-time Assessment". We offer the following definition for BES Cyber System:BES Cyber System - One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could cause a BES Disturbance or impact the Real-time Assessment capability, Real-time control and operation, or materially impact situational awareness of the BES.Situation awareness is somewhat vague and may mean different things to different people. The team should consider taking the description of situational awareness as shown in Attachment I - "Functions Essential to Reliable Operation of the Bulk Electric System" and making it a NERC Glossary of Terms definition.
2.54	LADWP	Disagree with scope	The 15 minute window is relative. The industry needs to define what is an acceptable time horizon.
2.55	Dairyland Power Cooperative	Disagree with scope	The 15-minute rule seems arbitrary and one dimensional. How does the availability of using a system for control relate to this time frame? I'm having trouble relating this to for instance a telemetry/control function. It would be possible that long periods of down time could pass without impact to the BES system... but under certain conditions it would be critical to have the monitoring and control functions.
2.56	Constellation Energy Commodities Group Inc.	Disagree with	The definition of a Disturbance includes a concept, as applied by Balancing Authorities of sudden failures of generation or interruption of load. The fifteen minute window is generally viewed as the length of time in which recovery should take place. The drafting

#	Organization	Yes or No	Question 2 Comment
		scope	team should look at narrowing the time horizon further to capture BES Cyber Systems that will directly control equipment and result in immediate system impacts. The definitions of Disturbance and Emergency reflect events that immediately impact the system; the fifteen minute window is viewed as the point in time by which the system should be recovered.
2.57	Constellation Energy Control and Dispatch, LLC	Disagree with scope	The definition of a Disturbance includes a concept, as applied by Balancing Authorities of sudden failures of generation or interruption of load. The fifteen minute window is generally viewed as the length of time in which recovery should take place. The drafting team should look at narrowing the time horizon further to capture BES Cyber Systems that will directly control equipment and result in immediate system impacts. The definitions of Disturbance and Emergency reflect events the immediately impact the system, the fifteen minute window is viewed as the point in time by which the system should be recovered.
2.58	San Diego Gas and Electric Co.	Disagree with scope	The phrase "real-time" doesn't have a definitive industry-wide connotation, although for collecting field data it usually means seconds instead of minutes. In general, SDG&E supports the inclusion of real-time operations systems being in-scope, but we support a shorter operational time horizon (such as 5 minutes) to make the definition more immediate, with more high value BES Cyber assets being part of the scope.
2.59	Minnesota Power	Disagree with scope	The scope of applicability and operational time horizon of 15 minutes appears arbitrary and Minnesota Power is unsure as to how the Standards Drafting Team envisions that a Registered Entity will be able to show and document (i.e., prove for audit purposes) that a particular Cyber System will or will not have an effect on the BES in a certain time period. If the intent is "real-time operations," then state that and drop "within 15 minutes."
2.60	Consultant	Disagree with	The scope statement should clarify the inclusion or exclusion (or alternative treatment) of backup systems, development systems and environments, quality assurance systems and environments, testing systems and environments.As stated the only systems that

#	Organization	Yes or No	Question 2 Comment
		scope	appear to be "in scope" are live production systems.
2.61	US Bureau of Reclamation	Disagree with scope	This requirement puts a premium on the definition of what the BES is. There are components of the power system that are not "BES" and therefore do not qualify under these Standards. This issue needs to be further addressed. Further, the term "operational time horizon" needs further definition. Is this 15 minute criterium to be applied under normal operation conditions, or only those that COULD be experienced if the Cyber System were to be compromised?
2.62	Ameren	Disagree with scope	We disagree with the scope; the 15 minutes should only apply if the disturbance is not recoverable.
2.63	Southern Company	Disagree with scope	While we understand the intent of the 15-minute scope, we feel that the inclusion of this factor causes too much vagueness in the interpretation of the definition. We recommend that the focus be limited to real-time operations only.
2.64	Verizon Business	Agree	The “15 minute” criterion needs to be expanded – perhaps in an associated guideline or “Frequently Asked Question”

3. **Requirement R1 of draft CIP-010-1 states, "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES to identify BES Cyber Systems for the application of security requirements." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

Many entities expressed concerns on the broad implication associated with the phrase "execute or enable…". Entities generally agreed with the assignment of compliance responsibility to owners, but many others expressed concerns for jointly owned facilities or facilities that may be operated by other than owners. There were many concerns expressed about the Functions and their description and definition. Others expressed concerns about the differences between systems and their components.

CIP-010-1 Requirement R1 has been replaced by CIP-002-5, which reads:

Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems*. All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

Additional guidance for jointly owned facilities has been provided in the Application Guidelines section of the standard. The reliability functions have been redefined as Reliability Operating Services to avoid any confusion with the use of the term Functions as used in the Functional model.

#	Organization	Yes or No	Question 3 Comment
3.2	WECC		Agree with the concept however, "...to execute or enable..." or "...which execute and/or enable." "to" can be construed as passive. It is redundant to utilize the phrasing "...to identify BES Cyber Systems for the application of security requirements."The following rewrite is proposed;R1. Each Responsible Entity shall identify and document each BES Cyber System(s) that it owns, which execute and/or enable one or more functions defined in CIP-010 - 1 Attachment I - Functions Essential to the Reliable Operation of the BES. (Violation Risk Factor: High)
3.3	Entergy	Agree	Agree that applicability should be strictly focused on "owned" assets.

#	Organization	Yes or No	Question 3 Comment
3.4	US Army Corps of Engineers, Omaha Distirc	Agree	Agree with R1 requirement - Find the measures for R1 - R3 troublesome. Measures are stated in terms of number of BES cyber systems. It is conceivable that plant SCADA systems could be considered a single system or a group of a few systems. How is a missed component handled? Is it another system or is a component. It appears like the violation measures are being handled as a count of BES cyber system components not BES cyber systems. Feel the measures should be revisited with the low number of systems likely to be identified in mind. Seems odd that any additional system is a sever violation if you have identified fewer than 6 systems.
3.5	Florida Municipal Power Agency	Agree	Although FMPA agrees with the requirements, FMPA suggests that naming Attachment I "Functions ...." will add confusion with the "Functional Model". FMPA suggests renaming Attachment I to "Activities Essential to the Reliable Operation of the BES", and of course modify R1 to reflect this change. Additional comments on Attachment I are included below in Question 6.
3.6	Garland Power and Light	Agree	Definitely agree with the words "it owns"
3.7	SCE&G	Agree	Guidelines should be provided to assist entities in determining how BES Cyber System Components should be grouped into BES Cyber Systems. Can a single component reside in two cyber systems?
3.8	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
3.9	Reliability & Compliance Group	Agree	Is the assumption that the initial list needs to contain both BES and non-BES Cyber Systems? It would be better if the standard was even more proscriptive here.
3.10	Con Edison of New York	Agree	Please note comments to question 6. It may be easier if the DT reference functions as detailed by FERC-approved NERC Reliability Standards. The definitions in Attachment I will ultimately lead to many requests for interpretation. R1 requires identification and documentation of BES Cyber Systems. There is no requirement to identify BES Cyber

#	Organization	Yes or No	Question 3 Comment
			System Components within CIP-010. However, CIP-011-1 R23 requires that you develop an inventory of these Components. Should this be a CIP-010 requirement? Then CIP-011 can expand on the Change Management Controls.
3.11	San Diego Gas and Electric Co.	Agree	SDG&E agrees with the wording in R1, but has additional comments and requests for clarification. Specifically, we request clarification regarding the "situational awareness" reference in Attachment I. In our case, as many other entities, we use Remote Terminal Units to gather data from BES substations and present that data to the operators to improve their Situational Awareness. Loss of a single RTU vs. loss of multiple RTUs affects the presentation of this data to operators to varying degrees (with associated effects on monitoring the BES), but the Standards don't address quantitative issues such as this.In a similar vein, SDG&E also requests clarification regarding the term "inter-entity real-time coordination and communication" in Attachment I. For example, are inter-entity telephone systems in-scope or is this referring to electronic data exchange between entities such as ICCP data links?Probably SDG&E's largest concern with CIP-010-1 R1 is the sheer amount of effort and resources it will take to build the lists of BES Cyber Systems and the impact categorizations. While there are some loose parallels with the current CIP-002 Standard, we won't be able to re-use the bulk of the work already done in our Risk-Based Assessment to identify Critical Cyber Assets. SDG&E's opinion is that CIP-010 doesn't leverage as much of CIP-002 as we'd like to see. We'd like to take advantage of what already has been produced to become Compliant with the existing Standards, and we see these new draft Standards as going in a new direction with many of the requirements. We would feel better about it if the new Standards were bringing substantial additional reliability and security to the BES, but that is not apparent.
3.12	Minnesota Power	Agree	With the previously stated recommendations regarding the definition of BES Cyber System (see Question 1.b.) and the changes indicated below, Minnesota Power generally agrees with the proposed Requirement R1. "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns which execute or enable one or more functions defined in CIP-010 - 1 Attachment I, Functions Essential to the Reliable

#	Organization	Yes or No	Question 3 Comment
			Operation of the BES, for the purpose of applying the security requirements."
3.13	BCTC	Disagree	- Recommend removal of the “Inter-Entity Real-Time Coordination and Communication” (Attachment 1) point as this is covered under the COM domain
3.14	Bonneville Power Administration	Disagree	"...that it owns to execute or enable..." is somewhat unclear. It appears the intent is the equivalent of "that it owns that is able to execute or enable...". As it is written, it can give the impression that the purpose of owning the system is to execute or enable the functions. That is too narrow. Another possible interpretation is that the "to execute or enable..." refers to the objective of the requirement. If that is so, then please break the objective out separately:"Objective: To execute or enable...Requirement: Each Responsible Entity..."Many of the other requirements include "to..." at the end of the requirement. These are clearly objective statements. They should be broken out separately, into an "Objective" and "Requirement", as stated above. The last phrase in Requirement 1 is “for the application of security requirements.” In Requirement 2 the last phrase is “for the application of Cyber Security requirements . . . .” Are these two phrases supposed to have the same meaning? If so, shouldn’t they use identical words? If not, what does “for the application of security requirements” mean? Is it referring to some or all of the requirements in CIP-011-1? If so, it should clearly state that and, if not the entire standard, which specific requirements it is referring to.It seems that it should read as follows: “for the application of the Requirements contained in Standard CIP-011-1.”
3.15	Consultant	Disagree	1. I think the standards should provide some distinction between ownership responsibility and operations responsibility, or provide a mechanism to identify the responsibility for the requirements based on each specific situation. (Technical Feasibility Exception for owner versus operator responsibility?) This may include split responsibility for different aspects of the requirements. (This comment probably applies to more than just this requirement in both CIP-010 and CIP-011.)2. Wording is confusing regarding systems for application of security requirements. Suggest ending the requirement statement after "...Reliable Operation of the BES."3. Suggest using the complete title of

#	Organization	Yes or No	Question 3 Comment
			Attachment I: "Bulk Electric System" not "BES".4. In all locations in both CIP-010 and CIP-011 suggest removing references to specific revisions (e.g. CIP-010-1). This requires all standards to be changed for a change in any one standard. The documentation of which revision was used at the time of implementation should be included in the Responsible Entity's documentation or compliance.
3.16	Dairyland Power Cooperative	Disagree	A Responsible Entity should be responsible for any systems used for their operation regardless of ownership. Basing responsibility based on the ownership of a system creates a big loophole. It is possible an interfacing utility or service provider could be involved. Basing responsibility on the ownership of the facility containing the systems make more sense.
3.17	Duke Energy	Disagree	Additional clarification is needed on the process for identifying and categorizing BES Cyber Systems. Requirement R2 should really come first, and require that Responsible Entities identify their BES Cyber Systems that meet the criteria in Attachment II (i.e., that can affect operations for the listed facilities/functions). Requirement R1 should come second, and require documentation of the functions affected for each BES Cyber system identified. Attachment I is not needed as part of the standard, but should be included in a guidance document.Much more clarification is needed to Attachment I. As described, the functions are far too broad. Specific language issues: o Monitoring & Control - Activities, actions and conditions that provide both monitoring and control of BES elements. o Situational Awareness - too broad as stated. Should be limited to situational awareness of the BES required by System Operators to perform their reliability-related functions o Inter-Entity Real-Time Coordination and Communication - too broad as stated; would seem to possibly include telephone lines
3.18	Arizona Public Service Company	Disagree	Additional verbiage needs to be included in order to clearly delineate which entity is responsible for an asset/system when it is jointly owned. Is it the majority owner? The operator? Where is the line?”

#	Organization	Yes or No	Question 3 Comment
3.19	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Again, no defining metrics. Small DP/LSEs will unnecessarily be required to comply with no BES reliability return.
3.20	IRC Standards Review Committee	Disagree	At the NERC CIP workshop in May 2010, there were so many examples brought forth where it could not be determined with exactness which components are part of a BES Cyber System or not because of the flexibility built into the requirements. "It depends" was often the response from the panels. So although the intent of CIP-010 is to provide more concrete guidance for registered entities to define BES Cyber Systems, in practice it may introduce just as many new questions about applicability as it may solve. It would be better to develop a performance based approach to define BES Cyber Systems rather than use bright line definitions to identify BES Cyber Systems. The proposed definitions of High and Medium include criteria that describe facilities, by KV level, MW size etc. But these are really proxies for an underlying intent of trying to describe a certain level of operational performance. For example, higher KV levels are assumed to reflect greater impacts on neighbors. And higher MW levels of generation are assumed to reflect greater risk of disturbance to load. Rather than use these proxies, the ratings High and Medium should instead employ descriptors related to a desired level of performance, for example, "...a loss of a facility that does not cause a IROL violation two systems away." Such an approach in defining the BES Cyber System would better focus the CIP-011 requirements and compliance efforts of both NERC and the registered entity on only those components that truly have a significant impact on the interconnected BES and not include facilities and components that although meet a bright line definition, really have minimal impact on the BES because of its particular location or configuration.
3.21	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
3.22	ERCOT ISO	Disagree	Comments: It should be stated that the Responsible Entity is allowed to perform R1 and R2 in the order they deem appropriate. Consider: "Each Responsible Entity shall

#	Organization	Yes or No	Question 3 Comment
			document each identified BES Cyber Systems that it owns which support the functions defined in CIP-010-1 Attachment I - Functions Essential to the Reliable Operation of the BES, for the application of security requirements.”
3.23	LCEC	Disagree	Concerned with the word "owns". Recommend "owns or operates" or a statement referencing operational responsibility.With the current definition of BES Cyber System Components including "one or more" devices, a lot of guidance will be needed to determine what constitutes a system versus a number of components. Most of the standards currently reference the system versus the component which could leave a gap in applicability. Is it assumed that all components must be a system or part of a system? Modifying the BES Cyber System Component definition to exclude "one or more" will help but entities will still need clarification on the grouping of components to form systems. An implementation guideline will help address this.
3.24	Constellation Power Source Generation	Disagree	Constellation believes that this requirement is too broad in terms of auditability. The proposed verbiage of CIP-010 is flexible in terms of how to define cyber systems, but is it implying that a methodology is needed to identify cyber systems? Or is it implying that each Responsible Entity define cyber systems as they see fit, without an explanation? For a company such as Constellation, which owns a fleet of diverse generation facilities, this flexibility will cause each plant to have its own unique methodology for developing cyber systems, which vastly increases the procedural burden of this standard when compared to the current version of CIP-002. A suggestion would be to clarify this requirement in a guidance by stating whether or not a methodology is needed to define cyber systems, and if not, what type of evidence would be suggested for showing that a cyber system has been identified correctly.
3.25	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy does not agree with the direction of the SDT and believes it is pre-mature to discard the current CIP requirements with a completely new philosophy. Most entities are in the compliance phase of implementation of the current CIP requirements and have yet to be audited. To have a fundamental shift in approach before the current requirements have been evaluated as to effectiveness and

#	Organization	Yes or No	Question 3 Comment
			compliance is unwarranted. In addition, CenterPoint Energy does not agree with the expansion of the CIP requirements to facilities that do not have a high impact on the reliable operation of the Bulk Electric System. CIP-010-1 and CIP-011-1 would apply some cyber security requirements to facilities and systems that the draft Standard would identify as having a medium to low impact to the reliable operation of the Bulk Electric System. While CenterPoint Energy agrees that some set of minimal security criteria should be used to protect facilities from malicious behavior, vandalism, or simply the curious, CenterPoint Energy believes these efforts are more accurately characterized as Good Business Practice and as such should not be auditable under mandatory reliability standards. Stated another way; those facilities and systems that have been identified as medium to low impact, using the draft standard methodology, by the nature of having little or no impact to reliable operation of the Bulk Electric System, should not be protected under auditable, mandatory, requirements.
3.26	Constellation Energy Control and Dispatch, LLC	Disagree	Disagree based on concerns with Attachment 1 Propose definitions for Attachment 1:Dynamic Response functions: BES equipment that reacts automatically to a BES Disturbance.Balancing Load and Generation: BES equipment that directly controls generation or load.Controlling Frequency: BES equipment that directly controls frequency (Does control of generation already cover this function?)Controlling Voltage: BES equipment that directly controls reactive power resources.Managing Constraints: (Delete this function) - Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Monitoring & control: Delete Monitoring and limit the BES equipment that control actions such as open and closing switches or relays, motor starts/stops, etc. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope

#	Organization	Yes or No	Question 3 Comment
			for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Restoration of BES: BES equipment required for system restoration.Situational Awareness: (Delete this function). Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Inter-Entity RT Coordination and Communication: (Delete this function) As written this function is too broad and should be limited data that drives operation of BES equipment . Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.
3.27	Constellation Energy Commodities Group Inc.	Disagree	Disagree based on concerns with Attachment 1Propose definitions for Attachment 1:Dynamic Response functions: BES equipment that reacts automatically to a BES Disturbance.Balancing Load and Generation: BES equipment that directly controls generation or load.Controlling Frequency: BES equipment that directly controls frequency (Does control of generation already cover this function?)Controlling Voltage: BES equipment that directly controls reactive power resources.Managing Constraints:

#	Organization	Yes or No	Question 3 Comment
			(Delete this function) - Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Monitoring & Control: Delete Monitoring and limit the BES equipment that control actions such as open and closing switches or relays, motor starts/stops, etc. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Restoration of BES: BES Cyber System or Components required for system restoration.Situational Awareness: (Delete this function). Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment. Inter-Entity RT Coordination and Communication: (Delete this function) As written this function is too broad and should be limited data that drives operation of BES equipment. Cyber systems used for monitoring and/or situational awareness that do not actually control BES equipment should be out of scope for this standard because they are not going to

#	Organization	Yes or No	Question 3 Comment
			directly result in a Disturbance condition in real time. In many cases loss of communication processes and procedures would be applied in situations where there is a complete loss of such a tool. At a minimum the monitoring and situational awareness tools subject to inclusion as a BES Cyber System should be limited to systems that provide data for monitoring and/or situational awareness that will be solely relied upon to directly operate equipment.Define the term Situation Awareness and how it applies to BES Cyber System or components required for system restoration.
3.28	Dominion Resources Services, Inc.	Disagree	Dominion agrees with R1, but is concerned with the functions listed in Attachment 1. Please see Dominion's response to Question 6.
3.29	E.ON U.S.	Disagree	E ON U.S. notes the absence of any study to assess whether identifying and categorizing all BES Cyber Systems as required by R.1 provides for material enhancement of BES reliability relative to the current Critical Asset identification methodologies allowed under CIP-002. E ON U.S. is also not aware of any effort to objectively quantify the costs that will result from R.1. Given the likely significant costs to consumers it would behoove the SDT and NERC to make an effort to understand the costs and incremental improvement to BES reliability associated with the sweeping changes proposed in CIP-010, R.1.The proposal does not allow for "no impact" assessments to be determined through engineering evaluation or other approved methods. E ON U.S. believes it would be an improvement to include language similar to that in existing CIP-002 R1.2.
3.30	EEI	Disagree	EEI generally agrees with R1, however, all owners of jointly owned facilities may not be responsible for protecting the BES Cyber Systems. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1. As a result, the drafting team should clarify what is meant by "owns" (i.e. how should GOs and GOPs collectively assess BES Cyber Systems).
3.31	ReliabilityFirst Staff	Disagree	For clarity, ReliabilityFirst suggests the following revision to the language of this requirement, "BES Cyber Systems that the entity owns, operates, or is otherwise

#	Organization	Yes or No	Question 3 Comment
			responsible for. . .”
3.32	American Municipal Power	Disagree	I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
3.33	USACE HQ	Disagree	I disagree with the new approach the team is presenting of substituting the risk-based assessment methodology with a list of essential function without any support of why they are essential. Order 706, page 70 - 72, recognize the need for risk-based assessment methodology guidance, therefore recognizing that the use of a quantifiable methodology based on risk is the right way to assess criticality of assets or systems present in the community. To create a list of functions and stating that they are essential without having done some type of study looking into what are really essential functions supporting the BES are only limits the protection of each asset to what a small group of people think is critical without taking into consideration the individual circumstances each asset brings to the table. I suggest that either the team moves back to the original intent in CIP-002 versions 1 - 3 and re-institute the language of risk-based methodology to create the list of BES Cyber Systems OR the team does a risk-based study on the BES to establish the “functions essential to the reliable operation of the BES”.
3.34	Pepco Holdings, Inc. - Affiliates	Disagree	In general we agree with R1 when there is only one owner of a BES Cyber System. However we also agree with EEI’s comments that owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are

#	Organization	Yes or No	Question 3 Comment
			Transmission Lines and/or Substations that are owned by multiple parties but one party is responsible for the operation and maintenance. Suggest considering adding language to R1 to cover joint owned facilities (e.g. In cases of joint owned BES Cyber Systems, the assigned Responsible Entity or Entities shall...).
3.35	Southern California Edison Company	Disagree	It is not clear how this requirement differs from CIP-002, R3. While the description of CIP-011 states the intent to retire CIP-003 through CIP-009, CIP-002 would still be in place. It is also not clear how these CIP-010-1 and CIP-002 would work together.
3.36	SPS Consulting Group Inc.	Disagree	It is unclear how the list of Essential Functions in Attachment 1 correlates to the categorization in Attachment II, which does not mention essential functions. I believe that Attachment I can be deleted and that Attachment II is fully sufficient for the categorization exercise. The stated purpose of Attachment I to define the scope of the CIP standards is unnecessary because the CIP standards do not apply to functions, they apply to registered entities, which are quite clearly stated.
3.37	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
3.38	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's recommendation to change owner to the owner-operator that performs operations as described below:Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The owner-operator that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.39	Michigan Public Power Agency	Disagree	MPPA is one of many organization that are co-owners of facilities that do not maintain operational control of the facility. MPPA suggests that the word "owns" in "...Systems that it owns to execute..." be changed to "operates."
3.40	Tenaska	Disagree	No R1 should be to identify BES assets that cyber systems are a part of. Consider

#	Organization	Yes or No	Question 3 Comment
			replacing attachment 1 with better definitions in the body of the standard.
3.41	Progress Energy (non-Nuclear)	Disagree	One major issue is that we do not have a clear definition of the BES. How do we define the BES? Is it all lines over 100kV excluding transmission feeders? It appears that some reliability groups are presently trying to define the BES clearly. If the BES includes >100kV import/tie lines, nuclear off-site power path, cranking path, quite a few T/T substations with microprocessor relays on lines could be put in scope of identification. These might be excluded or classified low impact if no communication is provided. Will power line carrier, transfer trip, etc. be in scope? This could turn into a very large list to develop and maintain.
3.42	Allegheny Energy Supply	Disagree	Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.43	Allegheny Power	Disagree	Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.44	PacifiCorp	Disagree	PacifiCorp agrees with EEI's recommendation to change owner to entity that performs operations as described below:Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is should be identified as responsible for the requirements identified by CIP-010-1.
3.45	Regulatory Compliance	Disagree	Please clarify - Attachment I - The function identified for Inter-entity Real-time Coordination and Communication: Is the coodination between the Responsible Entities' associated System operators or between BAs? Also what specific equipment is brought

#	Organization	Yes or No	Question 3 Comment
			into scope? Is it only for data communcation or voice communication as well?
3.46	Puget Sound Energy	Disagree	Puget Sound Energy feels that, without clarity (as commented in question 2 above), the scope of BES Cyber Systems can not be uniformly agreed upon and, as such, defendable metrics to prove compliance will not be able to be establish. For example, corporate email can be used to provide efficient communications between operators of the BES. The loss of corporate email, which in no way could cause a disturbance to the BES (and is physically and logically separated from all BES Cyber Systems), could "restrict" or "affect" the real-time operations of the BES through degradation in efficient communications. As well in order to prove compliance the unintended consequence of this requirement is a massive work effort to evaluate all the BES Cyber Systems in order to then establish or demonstrate which enable or execute essential functions.
3.47	Alliant Energy	Disagree	R1 is ambiguous when referring to "Joint-Owned Units", and we believe that the word "owns" should be replaced with "owns and operates." In a joint-owned facility, the operator typically has responsibility for compliance with NERC standards.
3.48	Wolverine Power	Disagree	See comments listed for 1.a
3.49	NextEra Energy Corporate Compliance	Disagree	See comments to 1a. In addition, NextEra believes if the introduction of "functions" is another area that could lead to misunderstanding. If left, we recommend it only be for "informational purposes" and not controlling. As stated above, the specific list of components in BES Cyber Systems of Control Centers, Generators and Transmission should be what is controlling and protected. Also, as the drafting team will see throughout these comments, language that can be misunderstood will be proposed to be changed. The drafters often spoke of their intent, and while this term is widely used by the industry and it always means well, it is not a compliance/regulatory term the serves the industry, NERC or FERC well. The intent of the drafting team is not recognized as record evidence, nor is it controlling in an audit or before NERC or FERC. Thus, preambles should be clear. For example, "Purpose: To provide clear understanding of what BES Cyber System Components must be protected consistent with CIP-011-

#	Organization	Yes or No	Question 3 Comment
			1.”Similarly, NextEra is not supportive of using technical guidance papers to supplement the Standards. NextEra believes the Standards are what NextEra will need to comply with and the guidance papers, unless approved by FERC, are not controlling from a compliance perspective. Moreover, guidance papers tend to be loosely written and subject to being misunderstood. NextEra would rather see the specifics in the Standards.
3.50	MWDSC	Disagree	Situational Awareness is a new term that will be confused with Monitoring and Control function in Attachment I. The term "Control and Operation" was changed from prior draft to "Monitoring and Control". Shouldn't situational awareness be performed by the same operator? Suggest deleting Situational Awareness and revising the Monitoring and Control function as follows:"Activities, actions and conditions that provide monitoring and control of BES elements, including the assessment of current, expected, and anticipated state of the BES.
3.51	Matrikon Inc.	Disagree	Still open for interpretation, in its most simple form the only action words are “execute” or “enable” that correspond the cyber system to each of the functions. Please provide further definition or guidance on its application.
3.52	Southwest Power Pool Regional Entity	Disagree	The ability of the entity to group its cyber assets into cyber systems as it sees fit potentially offers an opportunity to game the system by dissecting legitimate cyber systems into smaller groups of components with less span of control and thus lower impact. There needs to be some sort of sufficiency criteria to ensure proper logical grouping. Additionally, a concern to the auditor is the ability to ascertain that the entity has identified all of the pertinent cyber systems and that all of the necessary cyber system components have been accounted for. Lastly, consider modifying the phrase “...that it owns to execute or enable...” to read “...that it owns to execute, enable, or support...”
3.53	APPA Task Force	Disagree	The APPA Task force disagrees with the proposed requirement but we offer the following suggestions:We suggest that naming Attachment I “Functions ....” will create

#	Organization	Yes or No	Question 3 Comment
			confusion with the "Functional Model". We suggest renaming Attachment I "Activities Essential to the Reliable Operation of the BES", and of course modify R1 to reflect this change. Additional comments on Attachment I are included below in response to Question 6. There are many different business models in our industry, and "ownership" may not mean "owns and operates." Therefore we would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has any control of the BES Cyber Systems installed, and/or the related day-to-day compliance with NERC standards.
3.54	Nuclear Energy Institute	Disagree	The current CIP-002 provides a risk-informed approach to the identification of assets critical to the reliability of the bulk-power system. The current practice is for a generator owner/operator to coordinate with the local transmission owner/operator to determine if the generator is critical to maintaining the reliable operation of the Bulk-Power system.The proposed CIP-010-1 eliminates this risk-informed approach, and would require all generators of any size to be required to comply with the CIP Standards even if the BES would not be adversely affected by the loss of the generating facility.NEI believes that the proposed methodology in CIP-010-1 is contrary to the intent of section 215 of the Federal Power Act (FPA) (16 U.S.C. 824o) which is to prevent instability, uncontrolled separation, or cascading failures as the result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.In order for CIP-010-1, R1 to be acceptable, reliance on an analysis by the transmission system owner/operator must be performed to determine if the generator operator/owner facilities are critical to the reliability of the bulk-power system.
3.55	GTC & GSOC	Disagree	The definition unnecessarily restates detail that should be in the definition of BES Cyber Systems. We recommend it be simplified to state the following "Each Responsible Entity shall identify and document each of its BES Cyber Systems in order to apply Cyber security requirements."

#	Organization	Yes or No	Question 3 Comment
3.56	FirstEnergy Corporation	Disagree	The definitional terms for Control Center, BES Cyber System and BES Cyber System Components in conjunction with the Requirement R2 "Impact Categorization (Attachment II)" should provide sufficient direction to the "programmable devices" that are within in scope and require protection under the proposed CIP standard. The R1 requirement places an unwarranted compliance documentation burden on the industry with questionable reliability payback. FE suggests that R1 and its corresponding Attachment I can be eliminated from the standard.Secondly, the requirement describes two unique actions - identify and document - BES Cyber Systems. "Documenting" the identified BES Cyber Systems is actually evidence of compliance that should be left to the Measures and not explicitly stated in the requirement. Failure to identify a BES Cyber System poses a real reliability risk to the BES, however, identifying and protecting a BES Cyber System but only neglecting to include it in a documented report is an administrative task with no reliability risk.
3.57	USACE - Omaha Anchor	Disagree	The owner may be a distant owner - I feel it should be operators - or the owner in conjunction with the operator.
3.58	Detroit Edison	Disagree	The phrase "to identify BES Cyber Systems for the application of security requirements" at the end of R1 is a restatement of the purpose of CIP-010 and should be removed. Consider changing R1 to: Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010-1 Attachment I - Functions Essential to the Reliable Operation of the BES.
3.59	Indeck Energy Services, Inc	Disagree	The R1 requirement ignores the risk based assessment methodology that is required by FERC-see Order 706. [suggested replacement language] "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions, defined in CIP-010 - 1 Attachment I - Functions Essential to the Reliable Operation of the BES, and perform a risk assessment according to its risk based assessment methodology of the impact on the reliability of the BES to identify a BES Cyber Systems for the application of security requirements."

#	Organization	Yes or No	Question 3 Comment
3.60	US Bureau of Reclamation	Disagree	The unclear definition for "could have an effect on real-time operation..." as used in the opening of Attachment I, needs to be clarified/quanitized or defined. Almost any of these functions (and many more), at any facility - no matter the size - could have an effect. The effect needs to be characterized as more than trivial to be deemed essential to reliable BES operation. Whether the changes are made to the Attachment or within this requirement is immaterial. The language in the requirement needs to be cleaned up as follows: "Each Responsible Entity shall catgorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachement II - Impact Categorization of BES Cyber Systems." The title of Attachment to is incorrect in the requirement.
3.61	Platte River Power Authority	Disagree	There can be some confusion regarding who is responsible for implementing and demonstrating compliance with the CIP standards under certain circumstances (e.g. joint ownership). It would be helpful if there was a mechanism to identify the “Responsible Entity” responsible for implementing and demonstrating compliance for various Assets. The “Responsible Entity” designation could also include operators and could vary based on standard\requirement. For example:The designated Responsible entity is the owner unless specified otherwise.For Assets where an owner is not the designated Responsible Entity:- The owner must document an agreement with the designated Responsible Entity including the Asset(s) and requirements the designated Responsible Entity is responsible for.- The designation must be to a NERC Registered Entity.- The designation must be reviewed and reaffirmed annually
3.62	Manitoba Hydro	Disagree	This is satisfactory if identifying the cyber system with a reasonably short descriptive overall functional summary is sufficient. It is unsatisfactory if each and every single component of the cyber system must be described in some detail. Since some of the requirements in CIP-011 are at the BES Cyber System Component level, the need to identify the components should be explicitly required in the standard. Requirement R1 is unclear as drafted. It is not clear if the phrase “to execute or enable one or more functions...” describes the purpose of identifying BES Cyber Systems, or if it describes a

#	Organization	Yes or No	Question 3 Comment
			necessary characteristic of the BES Cyber Systems. Note that in Measure M1, "to" is replaced with "that", creating an inconsistency between Requirement R1 and Measure M1. Measure M1 is not a complete sentence. What needs to be documented?.
3.63	Southwestern Power Administration	Disagree	Though identification of BES Cyber Systems may be beneficial, adding prescriptive categories such as those included in Attachment I only add another layer of administrative "check-listing" for compliance purposes and do not actually have a positive effect on reliability. If Attachment I is intended as guidance in understanding the functions essential to reliable operation of the BES, it would be more appropriately included in a guidance document.
3.64	Midwest ISO	Disagree	We do not believe that it is necessary to document what function its BES Cyber Systems perform in attachment I. We believe that it is only necessary to test them against the criteria established in Attachment II. Developing inventory lists of what BES Cyber Systems performs what functions in Attachment I would increase the risk of a coordinate attacks should the information get into the wrong hands.
3.65	We Energies	Disagree	We Energies agrees with EEI comments. Owners of jointly owned facilities may not be responsible for BES Cyber Systems to be protected. For example, there are many Generating Units that are owned by multiple parties. The entity that performs operations (e.g. the licensed operator of a generating unit) is responsible for the requirements identified by CIP-010-1.
3.66	Madison Gas and Electric Company	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards. Attachment 1 requires clarification.Balancing Load and Generation, Controlling Frequency (Real Power) and Controlling Voltage (Reactive Power) are Functions Essential to Reliability Operation of

#	Organization	Yes or No	Question 3 Comment
			the Bulk Electric System but do not contain the modifier of BES as in Monitoring and Control does. Is it implied that the listed functions are only those functions Essential to Reliability Operation of the Bulk Electric System? Please clarify.
3.67	MRO's NERC Standards Review Subcommittee	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards.
3.68	The Empire District Electric Company	Disagree	We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards.
3.69	Alberta Electric System Operator	Disagree	We find the current wording somewhat confusing. Consider rewording the sentence. As a suggestion, "...that it owns that executes or enables one of..."
3.70	Oncor Electric Delivery LLC	Disagree	We need more clarity (white paper) to assist in how utility equipment should be identified as components or systems. Is the relaying scheme at a single substation a "system" and all the individual relays are "components", or is the primary and backup relays for a single line terminal, bus, or transformer the "system" and the individual primary/backup relay is a "component". This is basic to the implementation of this standard and needs to more fully defined.

4. **Requirement R2 of draft CIP-010-1 states, "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II – Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.**

Summary Consideration:

The majority of the concerns raised in the comments were related to Appendix 2, the criteria used for categorization.

Specific concerns about categorization are addressed in the responses to Q7 and in the criteria which were approved by industry for Version 4 of CIP-002.

In CIP-002-5, this requirement has been consolidated with Requirement R1 of the previously posted CIP-010-1, to create CIP-002-5 Requirement R1 as follows:

Each Responsible Entity that owns BES Cyber Assets and BES Cyber Systems shall identify and categorize its High and Medium Impact BES Cyber Assets and BES Cyber Systems according to the criteria contained in *CIP-002-5 Attachment I – Impact Categorization of BES Cyber Assets and BES Cyber Systems.* All other BES Cyber Assets and BES Cyber Systems that it owns shall be deemed to be Low Impact and do not require discrete identification. *[Violation Risk Factor: High][Time Horizon: Operations Planning]*.

#	Organization	Yes or No	Question 4 Comment
4.1	WECC	Agree	Agree with the comment but it is unnecessary to utilize the phrasing "...for the application of Cyber Security requirements commensurate with the potential impact on the BES." The following rewrite is proposed;R2. Each Responsible Entity shall categorize and document such categorization for each BES Cyber System(s) identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1. (Violation Risk Factor: High)
4.2	LCEC	Agree	Agree with the intent of the requirement but need to clarify the content of the attachment.

#	Organization	Yes or No	Question 4 Comment
4.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
4.4	FirstEnergy Corporation	Agree	FE supports R2 and the Impact Categorization achieved through Attachment II. Attachment II provides much needed clarity, compliance certainty but most importantly a consistent application of the critical infrastructure required to be secured within the context of the proposed CIP requirements.Suggested improvements to Attachment II are provided in our Question 7 response.As described in Question 3 above FE believes that R1 and Attachment I are not needed within the standard and that terminology for Control Center, BES Cyber System and BES Cyber System Components is sufficient. Therefore, conforming changes would be needed in R2 for a removal of R1/Attachment I. For example, "Each Responsible Entity shall document an impact categorization of its BES Cyber Systems consistent with CIP-010 Attachment ...."Requirement R2 and its corresponding Attachment II provides no guidance on whether digital relays colocated at a Transmission Facility need to be treated as individual BES Cyber Systems. FE recommends that the team clarify that a responsible entity could generically reference "Digital Relay Protection System" as a BES Cyber System located at a particular Transmission Facility (substation). There should be no need to identify/document each individual digital relay as a separate and unique BES Cyber System. Rather, the digital relay would be viewed as BES Cyber System Component of the Transmission Facility protection system. This will simplify compliance documentation, particularly for devices that may be associated with a Low Impact categorization.
4.5	Dynegy Inc.	Agree	I agree but request additional detail examples be provided to determine specifically what these items are.
4.6	NextEra Energy Corporate Compliance	Agree	In general, NextEra is supportive of the high, medium and low impact approach. However, in response to question 7, NextEra addresses concerns of the low impact approach.

#	Organization	Yes or No	Question 4 Comment
4.7	Minnesota Power	Agree	In order to increase clarity, Minnesota Power recommends the following changes to the language of Requirement R2: "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II, Impact Categorization of BES Cyber Systems. Each BES Cyber System's impact category will require the application of specific Cyber Security requirements commensurate with their potential impact on the BES."Minnesota Power believes that if a Registered Entity can support the exclusion of specific criteria identified in Attachment II with study data, then the Registered Entity should be allowed to exclude such criteria from further analysis.
4.8	Puget Sound Energy	Agree	Puget Sound Energy agrees with the language in R2, provided the language in attachment II is addressed (comments provided in question 7).
4.9	Con Edison of New York	Agree	See comments on question 7.
4.10	Platte River Power Authority	Agree	Suggest Revising:Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems for the application of Cyber Security requirements commensurate with the potential impact on the BES.
4.11	Reliability & Compliance Group	Agree	The categorization seems pretty straight forward however, it appears that you will be now excluding lots of "BES Cyber Systems" that were identified as CCA's originally and now will be just medium impact BES cyber systems.
4.12	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	The Requirement is sound in and of its self.
4.13	Bonneville Power	Agree	There need to be definitions of "High", "Medium", and "Low" impact. Attachment II describes how to determine whether a system meets the criteria for one of the impacts,

#	Organization	Yes or No	Question 4 Comment
	Administration		but doesn't give an overall explanation of what they mean. The CIP-002-4 draft included level definitions and that was a good idea. That level of detailed definition is not required; that detail is in Attachment II. But, a general impact level definition is needed, for example:"High: Loss of availability of the system leads to an unacceptable risk to the BES. Medium: Loss of availability of the system has a direct impact on the BES.Low: Anything else"These definitions will be used in answering the various questions about the tables.The objective of this requirement ("to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.In Requirement 2 the last phrase is "for the application of Cyber Security requirements . . . ." The last phrase in Requirement 1 is "for the application of security requirements." Are these two phrases supposed to have the same meaning? If so, shouldn't they use identical words? If not, what does "for the application of Cyber Security requirements . . . ." mean? Is it referring to some or all of the requirements in CIP-011-1? If so, it should clearly state that and, if not the entire standard, which specific requirements it is referring to.It seems that it should read as follows: "For the application of the Requirements contained in Standard CIP-011-1 . . . ."
4.14	Western Area Power Administration	Agree	Why is Cyber Security capitalized?
4.15	Independent Electricity System Operator	Disagree	(i) Medium impact categorization is based on an arbitrary generator nameplate rating of 1000 MVA, or voltage level of 200 kV and number of lines, with no regard to actual impact. The same is true of Special Protection Systems. Thresholds should be determined according to studies or other criteria determined by the Reliability Coordinator. As currently drafted, these criteria would significantly reduce the MW currently identified as 'Critical Assets' and protected within our Reliability Coordinator

#	Organization	Yes or No	Question 4 Comment
			area. (ii) The 3 impact levels (H, M, L) create additional layers of management complexity to implement and maintain security processes and monitor compliance, with no commensurate improvement to reliability. Based on the proposed applicability of CIP 11 for H,M & L categories, it seems likely that the number of BES assets afforded the maximum level of protection will decrease from the current standards.
4.16	E.ON U.S.	Disagree	: CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems currently lists 14 "High Impact Ratings" of the categorization of the BES Cyber Systems. E ON U.S. proposes that the Standard include only Control Centers and Backup Control Centers in the High Impact Rating category; all other points listed in the High Impact Rating category should be moved to the Medium Impact Rating category, and all points currently listed in the Medium Impact Rating category should be moved to the Low Impact Rating category.
4.17	BCTC	Disagree	Â Recommend sample BES Cyber Systems be provided for each impact categorization to help guide UtilitiesÂ (Attachment 2) Cost should not be a consideration as the focus is the reliable operation of the BES(Attachment 2) the impact categorizations are good for directing Utilities on how to categorize their BES Cyber Systems ... nice job!
4.18	USACE HQ	Disagree	As same as for question 3, I disagree with the new approach the team is presenting of substituting the risk-based assessment methodology with a list of thresholds to assign risk levels to assets. Again, Order 706, page 70 - 72, recognize the need for risk-based assessment methodology guidance, therefore recognizing that the use of a quantifiable methodology based on risk is the right way to assess criticality of assets or systems present in the community. I suggest that either the team moves back to the original intent in CIP-002 versions 1 - 3 and re-institute the language of risk-based methodology to create the list of BES Cyber Systems OR the team does a risk-based study on the BES to establish real threshold levels to assing risk to the different assets and/or systems in the community.

#	Organization	Yes or No	Question 4 Comment
4.19	Entergy	Disagree	Asset categorization in Attachment II may be valid for any number of purposes, but cyber security is not one of them. Size does not matter in terms of potential adverse impact to the BES as a functioning whole from cyber threats. Connectivity and network navigability are what matter in terms of the ability to adversely affect the bulk electric system through cyber means. Size matters for grid engineering and nominal-state operational grid management, physical security attacks (e.g. terrorist attack), and destruction by weather conditions (e.g. tornado). The cyber attack surface salient to integrity of the BES as a functioning system is primarily where routable protocols (e.g., TCP/IP) are used to connect operating sites, e.g., substations to control centers, regardless of size. The correlation between asset size and potential risk to the functioning BES as a whole is a misapplication of an electrical engineering frame of reference to what is fundamentally a networked-computing security engineering problem. The current approach brings great numbers of asset sites in-scope for required application of cyber defense countermeasures where the threat does not warrant it, e.g., substations of any size that are only connected back to a control/data center using legacy serial communications lines. If the paradigm of size-based impact categorization is to remain in the final Standard, specific requirements also should be established for each different type of network connectivity employed between sites, i.e., routed, legacy serial, dial-up, wired/wireless LAN, etc. One size fits all requirements such as that currently drafted will require overkill in far too many instances relative to genuine threat. As written, the standards are binary in terms of applicability across the spectrum of size-based impact categories, resulting in unnecessary requirements for some asset sites, generally medium impact sites with serial line communications only. This approach is not supported by any evidence in the administrative record. By bringing a large number of low-risk asset sites (i.e., substations using legacy serial communication lines only) into the scope of the requirements, they are imposing significant costs which do not address the real risks. Conversely, too little emphasis in the Requirements is placed upon “low impact” sites where routable protocols are used, which present a clear and present danger for which heightened security measures are certainly warranted.

#	Organization	Yes or No	Question 4 Comment
4.20	Madison Gas and Electric Company	Disagree	Attachment 2 requires clarification. Criteria Number 1.3, per the NERC Glossary, Wide Area is: The entire Reliability Coordinator Area as well as the critical flow and status information from adjacent Reliability Coordinator Areas as determined by detailed system studies to allow the calculation of Interconnected Reliability Operating Limits. Please give and state the reference of “must run” and how entities should interpret what “must run” is. Must run is a market issue, and could be designated as must run but for only a week. Criteria Number 1.11, is the intent that the automatic aggregate load shedding be under a common control system as is stated in the current CIP 002 Standard? If that is the case, adding a comment to clarify the criteria would provide clarity as in criteria 1.2 "(if using a shared BES Cyber System)"?
4.21	IRC Standards Review Committee	Disagree	Attachment II - Impact Categorization of BES Cyber Systems does not recognize that there is another dimension of risk or impact that must be considered. The availability of alternative tools that provide the same functionality should be considered when categorizing these components (e.g. a High Impact BES Cyber System with a viable substitute could reduce it to a Medium Impact).
4.22	Garland Power and Light	Disagree	Attachment II 1.4 Should state that it is the Primary Black Start Unit and does not include the Next Start Unit.1.5 Multiple circuits between two substations should count as a single transmission line.General CommentNeed to add “scoping filter” as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states “typically excludes business, market function systems, and non real-time systems”, then it is a good scope and we would agree
4.23	Southern California Edison	Disagree	Attachment II defines the amount of generation under control as the rated capacity of

#	Organization	Yes or No	Question 4 Comment
	Company		the resource. This is not accurate for some systems which can only control the resource between certain points (e.g. minimum operational output [Pmin] and maximum operational output [Pmax]). This could drastically overstate the impact of the cyber system on the BES. For example, suppose that a cyber system controlled a generating resource with maximum capacity of 2,000 MW. According to attachment II, this would then categorize as "high impact rating". However, suppose further that the system can only control the unit between its Pmin and Pmax which are 1,500 and 2,000, respectively. This would place the system in a "low impact rating" according to the attachment. The Attachment II should be modified to account for only the capacity that can be controlled by the system.In addition, Attachment II designates as a high impact rating, "Each BES Cyber System that can affect operations for Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan." This should be clarified to show only BES Cyber Systems will be utilized during the period of time that the resource is providing actual Blackstart service. In SCE's case, if a Blackstart unit is on GMS during normal operating conditions, this should not make it a high impact rating in and of itself. If GMS will be used in the Blackstart plan to restore the system, then it should be included.
4.24	ERCOT ISO	Disagree	Comments: It should be stated that the Responsible Entity is allowed to perform R1 and R2 in the order they deem appropriate. Consider: "Each Responsible Entity shall document categorization of each BES Cyber System identified in Requirement R1. Categorization must address the criteria contained in CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems."
4.25	Tenaska	Disagree	Dependent on R1
4.26	Constellation Energy Control and Dispatch, LLC	Disagree	Disagree based on concerns with Attachment 2. Attachment 2, 1.1. As drafted BES Cyber Systems associated with generating facilities that have a Contingency Reserve obligation lower than their net Real Power capability would be forced to be in the High Impact Rating even though they may be only capable of producing 600 MW. I do not believe the drafting team is intending to capture generators at this capability level. I recommend

#	Organization	Yes or No	Question 4 Comment
			having a specific net real power generation threshold that could result in frequency decay to underfrequency load shedding levels and elimination of the term Contingency Reserve to ensure that a larger threshold is captured.Attachment 2, 1.8 1.8 Transmission Facilities and Generation Facilities are capitalized terms in parts of the draft but not defined terms in the NERC Glossary. Based on their use in the standard a definition should be established. For example, the debate on whether operation of generator interconnection facilities qualifies the operator for transmission operator status may lead to confusion as to who is responsible to categorize Transmission Facilities under this standard.Atachment 2, 1.12, 1.13, and 1.14 - delete and replace with the following: A Control Center that directly operate BES equipment to support the functions (as modified per suggestions) listed in Attachment 1, and whose operation could result in the loss of X MWs in the Eastern Interconnection, X MWs in the Western Interconnection or X MWs in the Texas and Quebec Interconnections. The Interconnection megawatt thresholds should be treated seperatly and not combined.
4.27	Constellation Energy Commodities Group Inc.	Disagree	Disagree based on concerns with Attachment 2. Attachment 2, 1.12, 1.13, and 1.14 - delete and replace with the following: A Control Center that directly operate BES equipment to support the functions (as modified per suggestions) listed in Attachment 1, and whose operation could result in the loss of X MWs in a balancing authorities' interconnection. The Balancing Authority megawatt thresholds should be treated separately and not combined.Request clarification and definition for the term Generation Aggregation and shared BES Cyber System.
4.28	Exelon Corporation	Disagree	Exelon does not agree with all of the specific criteria in Attachment II. Each of the criteria needs to either align with the other existing standard requirements, or have a technical basis or business risk mitigation basis to be defined as criteria. It would be very beneficial to the industry's understanding of each requirement if the basis for each was included in the Attachment or supporting documentation. One result of a deterministic criteria, in terms of a lost MW threshold and assuming all generators employing a common cyber system are lost "in combination" is that detailed studies of cyber impact on equipment are avoided. That is, it is no longer necessary to identify specifically which

#	Organization	Yes or No	Question 4 Comment
			critical assets are affected. With the change in paradigm, a simple identification that a cyber system is common to multiple generators will result in a determination of "High Impact".
4.29	Allegheny Energy Supply	Disagree	Generally agree with intent, however there should be a "None" category in addition to High, Medium, and Low. For example there are likely Cyber Systems on very small generators connected to low voltage transmission that could not have any adverse impact on the BES.
4.30	Oncor Electric Delivery LLC	Disagree	High, Medium, Low is not granular enough. An entity which operates a facility which has no IP based communication should not be required to comply with the cyber security requirements of this proposed standard.
4.31	American Municipal Power	Disagree	I disagree with the structure of CIP-010, but I agree with the intent. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
4.32	Progress Energy - Nuclear Generation	Disagree	If a plant system at a nuclear facility is in scope for NERC CIP Standards, additional categorization is not needed.
4.33	Public Service Enterprise Group companies	Disagree	In general there is agreement with the R2 text. However, in Attachment II, statement 1.4 entails categorizing all Blackstart Units with a "High Impact Rating", while statement 1.6 requires that only the "primary cranking path" transmission facilities need to be categorized with a "High Impact Rating". Statement 1.6 implies that some Blackstart

#	Organization	Yes or No	Question 4 Comment
			Units, although categorized with a “High Impact Rating” would not be afforded transmission facilities with the same risk categorization. We recommend changing statement 1.6 to include only Blackstart Units that are in the primary cranking path.
4.34	National Grid	Disagree	In lieu of the BES NOPR and the exemption process currently proposed, if facilities above 100 kV are exempted by NERC and FERC, will those facilities automatically be exempted from CIP standards? Currently, as per the standards, all the BES systems which are not categorized high impact or medium impact will be defaulted to LOW IMPACT category regardless of how the facility is impacting the Bulk power system. There are facilities >100kV having very localized impact and minimal impact to the reliability of the BES system for which entities will request for exemption. National Grid requests the SDT to clarify this issue.
4.35	Luminant	Disagree	Medium Impact: an item for TO, TOP, GO, GOP Functions performed at primary or backup control centers has been left off of attachment 2. This was in the previous posting as item 2.6"Control Centers and backup Control Centers controlling transmission ... This should be reinstated.
4.36	Matrikon Inc.	Disagree	My suggestion is that the term “system” is replaced with “component”, as that is how the security controls of CIP-011 will be applied (to individual cyber components). A typical control system is built of multiple components, and some are more important than others (eg. operator stations versus controllers). As a whole, they work together to control generation or transmission, and identifying impact of each component will help with the application of CIP-011-1.
4.37	Seattle City Light	Disagree	NERC should first assess the effectiveness of the existing standards before proposing replacements. The current Requirements haven’t yet had the chance to undergo a full assessment for effectiveness. The impact of adopting CIP Requirements was tremendous and forced utilities to develop and implement new operational processes at a great expense. The first round of CIP Spot Checks is just now underway and is providing the first validation point for interpretations of the standards (and our first

#	Organization	Yes or No	Question 4 Comment
			round of significant penalties.) Utilities are now at a pivotal point in maturing their CIP compliance programs. Drastically changing the requirements now is a common reaction to newly introduced regulatory compliance frameworks and NERC should learn from the mistakes of other regulatory bodies that now have mature compliance frameworks (i.e., PCI, HIPAA, SOX.) Opportunities to further mature and improve the effectiveness of our CIP compliance programs will not happen if the proposed methodology is adopted in the near future. The cost and resource expense will shift to adapting to the new standards which carries a significant opportunity cost from a risk perspective.
4.38	Duke Energy	Disagree	R1 and R2 should be reordered and reworded (see comment on Question #3 above). Also, the quantities identified on Attachment II appear arbitrary, and need an engineering basis. We suggest an approach based upon Violation Risk Factor language, such that for the High Impact Rating, the qualifier should be whether or not the BES Cyber System could directly cause or contribute to Bulk Power System instability, separation, or a cascading sequence of failures, or could place the Bulk Power System at an unacceptable risk of instability, separation, or cascading failures. For the Medium Impact Rating, the qualifier should be whether or not the BES Cyber System could directly affect the electrical state or the capability of the Bulk Power System, or the ability to effectively monitor and control the Bulk Power System, but is unlikely to lead to Bulk Power System instability, separation, or cascading failures.
4.39	San Diego Gas and Electric Co.	Disagree	SDG&E recommends aiming for a limitation of scope related to those assets that are truly high and medium impact categorizations. Some of the high and medium items could have “BES outage” implications but not necessarily result in instability of the BES. We recommend having consistency in the application of the assets included in the impact categories to the BES as a whole. Do the HIGH or MEDIUM impact categorizations consider redundancy and functionally equivalent back-ups? SDG&E recommends that this be taken into account during the categorization process.SDGE is concerned about the sheer number of assets that will be tagged “High impact” with the definitions presented in Attachment II, leading to a much larger compliance workload by entities with these new CIP Standards. Will all of these efforts bring significant additional

#	Organization	Yes or No	Question 4 Comment
			reliability to the BES?In paragraph 1.14, SDG&E has a concern about the last portion of the last sentence that reads "functionality that remotely controls a BES Cyber System with a High Impact Rating." That verbiage has the capability of causing many additional assets to fall in-scope that do not necessarily need to be. Suggest striking those words out of 1.14 since there are other protections in place within other requirements to protect the BES Cyber Systems with a High Impact rating.
4.40	Wolverine Power	Disagree	See comments listed for 1.a
4.41	Manitoba Hydro	Disagree	See comments to Question 3.
4.42	Indeck Energy Services, Inc	Disagree	The Impact Characterization of BES Cyber Systems is arbitrary and overly simplistic. It groups all facilities, regardless of the functions from Attachment I that they may or may not be able to perform and the significance of that type of facility to providing that function, in three arbitrary categories, LOW, MEDIUM and HIGH. The LOW category sweeps too broad a stroke. For generators, it arbitrarily includes, as a minimum, all generators less than 1,000 MW, regardless of type or capability to provide any or all of the functions from Attachment I. For example, one 150 MW generator providing "Controlling Voltage (Reactive Power)" has much less, probably a de minimis level, of support compared to a 999 MW generator. Wind generators are intermittent and non-dispatchable and, unlike dispatchable generators which are almost all running at high loads at high load times, when Controlling Voltage is a problem, are unlikely to be running near full load at those times. The categorization needs to be much more specific to the facility being categorized under CIP-010 and the function to be performed. Although the CIP-010 and CIP-011 are already voluminous, in order to positively affect BES ALR, they need to be restructured to reflect the complexity of the BES and not arbitrarily set LOW, MEDIUM and HIGH categories. [suggestion] There should be 5 categories: VERY HIGH, HIGH, MEDIUM, LOW and VERY LOW based upon the relative impact on the BES ALR, for each of the functions in Attachment I.

#	Organization	Yes or No	Question 4 Comment
4.43	PacifiCorp	Disagree	The initial wording “Each BES Cyber System that can affect operations for” should be clarified or additional clarification added to some of the following items. For example the wording above, together with the wording associated with 1.8 give fairly good guidance, but the wording applied to items 1.4 and 1.5 are not as clear. The wording “affect operations” can have many meanings ranging from minor operational issues to total loss of the facility. The phrase “singularlity or in combination” in Item 1.1 of Attachment II seems to be attempting to incorporate multiple units of an integrated plant, but the parenthetical does not effectively convey that concept. While item 1.1 ties back to the Contingency Reserve and the Reserve Sharing Group, it does not provide definitive guidance regarding which Facilities are meant to be incorporated into the requirement since this value is not easy to obtain and may by definition change year to year. Also, item 1.3 seems to be an “either/or” catch-all related to item 1.1, but there is no indication of who determines which units are “must-run” units. It is unclear how A BES Cyber System, if rendered unavailable, degraded, compromised, or misused, within 15 minutes, cause a disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES could fall into anything other than High or Medium impacts.
4.44	US Bureau of Reclamation	Disagree	The language in the requirement needs to be cleaned up as follows: "Each Responsible Entity shall catgorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachement II - Impact Categorization of BES Cyber Systems." The remaining parts of sentence should be deleted.
4.45	Detroit Edison	Disagree	The phrase “to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES” at the end of R2 is a restatement of the purpose of CIP-010 and should be removed. Consider changing R2 to:Each Responsible Entity shall categorize and document such categorization of each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II - Impact Categorization of

#	Organization	Yes or No	Question 4 Comment
			BES Cyber Systems.
4.46	Progress Energy (non-Nuclear)	Disagree	This is a good approach to apply protection based on an impact level vs. an all or nothing approach. The trigger levels (MW, MVar, etc) need to be reassessed - are these realistic / practical? This requirement is going to involve extensive effort and coordination between work groups. The DSCADA master that could control all T/D substation capacitor banks would be included. The term misused shows up a couple more times in Attachment II. It would appear that 1.11 includes the T/D Substation under frequency relaying. This is installed in almost every T/D substation which would require some level of access control.What is a generation facility versus a unit?Do we need to identify each cyber component of the BES Cyber System or just the (sub)system itself? Our interpretation of R1, R2, & R3 is that the requirements are driving us to identify Cyber subsystems. If we design small Cyber subsystem architectures we could get to Low impact categorization for each defined subsystems?Are the requirements aimed at subsystem level or overall system? An example would be to design a simple cycle Cyber system (Siemens T3000) architecture for combustion turbines alone and a second Cyber system (Ovation) for the balance of plant. We can make these independent systems at the process level and thereby minimize their respective impacts on the BES. Is that NERC's intent?
4.47	Southwestern Power Administration	Disagree	This requirement seems to be an excellent candidate for performance/results-based criteria rather than numerous bright line requirements that may or may not actually have a significant effect on the BES, depending on the surrounding topology, operating procedures, or configuration of a particular Responsible Entity.
4.48	MWDSC	Disagree	Unclear how much supporting documentation or explanation is required to demonstrate how your system applies or doesn't apply to each of the subcategories. For example, would a table with "yes", "no", or "not applicable" and certified by a SME be sufficient?
4.49	Turlock Irrigation District	Disagree	We agree with the principle of the Requirement, however, we disagree with some of the

#	Organization	Yes or No	Question 4 Comment
			High Impact Rating criteria in Attachment II, as explained in question 7 below.
4.50	Midwest ISO	Disagree	We do not believe the drafting team has developed a justification for moving away from the Critical Asset concept. We understand that the regulators have a concern about the level of Critical Assets identified but that could mean the criteria simply needs to be more stringent for selecting Critical Assets. If the categorization approach is maintained, at a minimum, a no or negligible impact category should be adopted. There are BES Cyber Systems that simply cannot have an impact on reliability and therefore the CIP standards should not apply to them.
4.51	Ameren	Disagree	We generally agree with the criteria used to identify "High" impact facilities, but believe that the item 1.5 criterion should be expanded to include EHV transformers, and not limited to 4 EHV lines. However, there are too many EHV facilities in item 2.6 that would be classified as "Medium" impact, but should be classified as "Low" impact. It is suggested that EHV facilities with three or less EHV lines and transformers should be considered as "Low" impact, as they likely have little impact on the BES.
4.52	Verizon Business	Disagree	In Attachment II, Item 1.1 regarding Generation Facilities, references to "Contingency Reserve" or "Reserve Sharing Group" should be removed. Specifically, any Generation Facility, singularly or in combination with aggregate higher than 2,000 MW, should be included as a High Impact Rating. Referring to the "Contingency Reserve" is confusing and could result in the incorrect or inconsistent declaration of a generation asset as a High or Medium impact.

5. **Requirement R3 of draft CIP-010-1 states, "To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall:**

   3.1 review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and categorization

   3.2 review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it owns

   3.3 update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES."

   Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many entities expressed concerns about the requirement to review the categorization following a planned change. Others expressed concerns again on the emphasis on ownership, but asked for the addition of "or operates".

In response to these comments, the requirement has been restructured, separating changes to the BES and categorization, and periodic reviews and approvals. More specificity has been added in the requirements as to when the categorization has to be updated upon a change. The SDT continues to believe that owners should be responsible for compliance and that the responsibility to operators should be the subject of agreements between the owners and operators.

#	Organization	Yes or No	Question 5 Comment
5.1	Progress Energy (non-Nuclear)		Agree that there needs to be a periodic review set cycle as well as a process to assess the impact for current projects. One concern could be how we deal with multi-phase projects that may extend over years.3.2 should not require that the whole identification and categorization process be redone for any 'planned changed'. Suggest changing the wording to 'review the identification and categorization of its affected BES Cyber Systems as a results of any planned change to the portion of the BES that it owns.'
5.2	MWDSC		Although R3 generally appears reasonable, cannot comment on specified times until all the requirements are finalized.

#	Organization	Yes or No	Question 5 Comment
5.3	National Rural Electric Cooperative Association (NRECA)		In R 3.3, please provide an explanation on "when applicable" -- explain this so that both the auditor and a registered entity can understand the "when applicable" circumstances.In R 3.3, what is meant by "such change" -- is it referring to actions related to R 3.1 and 3.2? If yes, ensure the standard is clear about this in order to minimize confusion about what is required.
5.4	Arizona Public Service Company		Potential confusion may exist without guidance or criteria that indicate how, specifically, a BES Cyber System Component should be identified. This is a problem of specificity in uniquely identifying a Component versus generically categorizing types of Components. This also relates to CIP-011 R23 and the inventory. Some potential options for specificity include manufacturer, model, serial number, assigned name or unique identifier, and location (logical and/or physical). Concerns with inventory management and uniquely identifying include how to better determine if a Cyber System Component has been modified or replaced with a different one, etc.
5.5	FEUS	Agree	3.2 is not clear when the entity is required to review the identification and categorization as a result of a planned change. 3.3 require documentation to be updated relative of changes from R1 and R2 within 45 calendar days. The drafting team should consider clarification for 3.2 either prior to implementation/completion of the planned change or within xx days.
5.6	Constellation Energy Commodities Group Inc.	Agree	Add a materiality component in 3.2.; review identification and categorization of BES Cyber Systems upon significant planned changes. Also recommend adding provisions for re-evaluating new systems prior to going live.
5.7	Constellation Energy Control and Dispatch, LLC	Agree	Add a materiality component in 3.2.; review identification and categorization of BES Cyber Systems upon significant planned changes.
5.8	WECC	Agree	Agree with the general requirements, but for clarity and auditability the following rewrite is suggested.R3 Perform a documented review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and

#	Organization	Yes or No	Question 5 Comment
			categorization. R4 Perform a documented review the identification and categorization of its BES Cyber Systems as a result of any planned or unplanned change to the portion of the BES that it owns.R5 Update or reaffirm the documentation specified in Requirements R1 and R2 within 45 calendar days from the completion of reviews as required by R3 and R4.Also suggest that the SDT consider requiring documentation be updated PRIOR to completion of the change.
5.9	Florida Municipal Power Agency	Agree	Although FMPA agrees with the intent of this requirement, we believe that 3.2 and 3.3 are duplicative and confusing from a monitoring perspective. We also note that there seems to be a gap for significant changes to BES Cyber Systems. In addition, ownership of BES Facilities seems to be the incorrect determining factor, especially since the definition of BES Cyber Systems is focused on operations and it would seem that the focus ought to be on the BES Cyber Systems owned by the System Operator to operate the BES within its operational scope. FMPA recommends deleting 3.3 and replacing 3.2 with the following:"3.2 Review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it operates. The effective date of any changes to BES Cyber System identification or categorization shall be the in service date of such change."Such language would result in the need to plan ahead of time and ensure the documentation is developed, but not necessary implemented until the in- service date of the new equipment.FMPA also recommends adding a new 3.3 to address significant changes to BES Cyber Systems that may impact identification and categorization, such as:"3.3 Review the identification and categorization of its BES Cyber Systems as a result of change in BES Cyber System configuration or scope. The effective date of associated changes to BES Cyber System identification or categorization shall be the in service date of such change."
5.10	Minnesota Power	Agree	Minnesota Power recommends the following wording change to increase the clarity of Part 3.2, "...as a result of any planned and implemented change..."
5.11	PNGC-Cowtitz-Central Lincoln-Benton-Clallam	Agree	Need to clarify what is required for temporary situations, such as a normal open closed to allow maintenance. The closing of the open would be a "planned change," but only

#	Organization	Yes or No	Question 5 Comment
	Group		temporary. The Change in status of a BES Cyber System would be a wasted compliance effort for only a short duration.
5.12	US Army Corps of Engineers, Omaha Distirc	Disagree	"planned change" in 3.2 needs to be qualified. Suggest changing to "planned change likely to alter the impact of the associated BES cyber systems." Changes to BES Cyber Systems that could change their impact on the BES should also be considered.
5.13	Covanta Energy	Disagree	3.1 - If no changes have been made to any BES Cyber Systems, would suggest changing review period from 36 months to 60 months.... need to reduce administrative activities to allow more focus on reliability based activities.
5.14	Duke Energy	Disagree	3.1 is part of change control. Do we still need this review? Also, 3.2 implies that ALL BES Cyber Systems would need to be reviewed as a result of any planned change to the portion of the BES that it owns. Need to bound this review to only BES cyber systems that are affected by the change.
5.15	Southwest Power Pool Regional Entity	Disagree	3.2 assumes that the BES Cyber System owner is also the owner of the BES assets being changed. This is not always the case. There are, for example, numerous instances where the Balancing Authority, Transmission Operator, and / or Generation Operator is not the Transmission and / or Generation Owner. Some sort of mandatory coordination is required to avoid this important requirement from falling through the cracks. 3.3 only requires a documentation update to be completed upon a change to the BES. This requirement should be modified to also require a documentation update upon a change to the BES Cyber System configuration, including adjustments to the list of components and supporting networks.
5.16	LCEC	Disagree	3.2 Change "owns" to "owns or operates". "Any planned change" may not be signficant enough to justify a full review.
5.17	Hydro One	Disagree	A local definition of “planned change” is needed. Suggest this definition excludes planned outages or maintenance. “Modification to facilities” as used in FAC-009 should

#	Organization	Yes or No	Question 5 Comment
			be considered.
5.18	Northeast Power Coordinating Council	Disagree	A local definition of “planned change” is needed. Suggest this definition excludes planned outages or maintenance. “Modification to facilities” as used in FAC-009 should be considered.
5.19	BCTC	Disagree	Â Preference would be to retain the current process of an annual review BES Cyber Systems and impact categorizationsÂ Please consider that if a change occurs that results in a BES Cyber System’s impact categorization increasing (i.e. from medium to high) the resulting effort to bring this system into compliance could be substantial (i.e. 6 to 12 months); how are these types of scenarios covered under Version 4?
5.20	USACE - Omaha Anchor	Disagree	A) 3.2 - any planned changes to the “cyber-system” portion of the BES that it owns. Otherwise you would be continually reviewing the plansB) 3.1 - would prefer to strike 3.2 and change 3.1 to 12 months.
5.21	Ameren	Disagree	Ameren feels that 45 days is too short and is also an uneven boundary that is hard to track. We would recommend changing it to a more even boundary such as bi-monthly (60 days) or quarterly (90 days). In the case of a complex merger or acquisition between responsible entities there needs to be additional guidance, longer timelines established, etc. to allow sufficient time before and/or after the completion of the transaction for compliance to be achieved and implies a perfectly complied with Configuration Change Management Program. Suggest adding “or as a result of the periodic review” at the end of R3.3.
5.22	E.ON U.S.	Disagree	CIP-010-1, R3.2 creates arguments that parties must constantly assess and re-assess their Impact Ratings of facilities. This is particularly true given that changes to the BES occur on a daily basis. Parties should be permitted expressly to engage in an annual assessment and a reassessment should only be required for “any major planned change to the portion of the BES that it owns prior to implementation of such plan.”CIP-010-1, R3.3 should read, “Update, when applicable, the documentation specified in

#	Organization	Yes or No	Question 5 Comment
			Requirements R1 and R2 within 45 calendar days of the completion of such major changes to the BES."
5.23	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
5.24	PacifiCorp	Disagree	Comments: The term "Any any planned change" used in 3.2 is terribly open-endedshould be more specific to avoid including small planned changes that have a de minimis impact on the identification and categorization of BES Cyber Systems. There must be some operationally prudent, de-minimus changes that can be made without triggering the 45 day change reviewIn addition, PacifiCorp suggests the following:. Change Modify item 3.3 to state Update documentation specified in Requirements R1 and R2 within 45 calendar days of any categorization changes caused by modifications to the BES.
5.25	Black Hills Corporation	Disagree	Define "change" in terms of those alterations to BES Cyber Systems which may modify the functional identification or an impact categorization. There are numerous minor changes which clearly will not change either Attachment I or II assignments and would not need to be tracked. If they are not tracked, an entity will not be able to prove compliance.
5.26	Exelon Corporation	Disagree	Exelon is concerned that this Requirement implies that each BES Cyber System Component will need to be classified as High, Medium or Low Impact. If this is the case, this will result in a major change management initiative with field personnel and add unnecessary administrative burden and expense with no resulting benefit to the reliability of the BES. Given that concern, Exelon suggest that Requirement 3.2 be modified to read "review the identification and categorization of its applicable BES Cyber Systems as a result of any planned change to the portion of the BES that it owns." Exelon has several concerns as to how this Requirement would be audited. As written, Requirement 3.2 could be interpreted to mean that ANY change to the BES, whether it impacted a BES Cyber System or not, would necessitate a 45 day review and documentation. Furthermore, what is the definition of "planned"? Exelon is concerned

#	Organization	Yes or No	Question 5 Comment
			that like-for-like emergent equipment replacements would likewise necessitate a 45 day review and documentation.
5.27	Dominion Resources Services, Inc.	Disagree	Extending the window for periodic validation of the identification and categorization of BES Cyber Systems is an improvement given the additional requirement to review the impact of planned changes. The current language implies that all identified and categorized BES Cyber Systems must be reviewed each time a change occurs to any single system, although the intent is only to determine the impact of the change. How that determination is made should be at the discretion of the Responsible Entity. The wording for R3.2 should be changed to more accurately represent the intent as follows:"...determine whether planned changes to the portion of the BES it owns, requires the identification of additional BES Cyber Systems or changes or impacts the categorization of any existing BES Cyber System."
5.28	ReliabilityFirst Staff	Disagree	For clarity, ReliabilityFirst suggests the following revision to the language of these requirements, 3.2 ". . . of any planned change to the portion of the BES that it owns or operates", 3.3 "Update within 45 calendar days, the documentation specified in Requirements R1 and R2 when the review required in 3.1 or 3.2 indicates a change."
5.29	MRO's NERC Standards Review Subcommittee	Disagree	For item 3.2, we believe the word "planned" should be replaced with "incorporated". Otherwise, an entity could end up identifying and categorizing BES Cyber Systems that never actually end up getting installed.
5.30	Oncor Electric Delivery LLC	Disagree	High, Medium, Low is not granular enough. An entity which operates a facility which has no IP based communication should not be required to comply with the cyber security requirements of this proposed standard.
5.31	American Municipal Power	Disagree	I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will

#	Organization	Yes or No	Question 5 Comment
			be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
5.32	Constellation Power Source Generation	Disagree	It seems the intent of R3.2 and R3.3 is to review and document any changes to a BES Cyber System that an entity owns, but instead it states "a change to the BES." An ownership change of a generation facility, or the change of an electromechanical overcurrent relay to a microprocessor overcurrent relay would change a BES Cyber System, but that doesn't change the BES. These requirements need to be rewritten to state BES Cyber Systems in place of BES.
5.33	Green Country Energy	Disagree	It would be nice to add a bit more definition to the timeframe. 3.1 within 36 months of last completed identification... 3.3 within 45 days of approved completion of such change...
5.34	Luminant	Disagree	Item 3.2 is unclear and very broad. Any planned change to the BES that it owns could simply be the changeout of an oil pump or boiler tubes. Luminant proposes two possible fixes. First, limit the review to changes that impact the BES Cyber Systems, or impact the High, Medium or Low rating. Even this is problematic in execution and enforcement. S
5.35	MidAmerican Energy Company	Disagree	Item 3.3 is not clear what does "update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES." mean. Change item 3.3 to state Update documentation specified in Requirements R1 and R2 within 45 calendar days of any categorization changes caused by modifications to the BES.
5.36	National Grid	Disagree	National Grid recommends a local definition of "planned change". Also, clarify if planned change refers to an "approved" change. There are scenarios when planned changes are

#	Organization	Yes or No	Question 5 Comment
			not approved by Senior Management for various reasons. Should the planned change still be “reviewed”? What about “unplanned changes”?
5.37	NextEra Energy Corporate Compliance	Disagree	NextEra suggests combining 3.2 & 3.3 as follows:3.2 For any planned change that results in a BES cyber system re-categorization (low, medium, high) the documentation specified in R1 & R2 will be updated within 45 days of the completion of such change.NextEra also suggest eliminating or specifically defining what constitutes a change that needs to be documented, such as a hardware modification, or change to network connectivity.
5.38	Progress Energy - Nuclear Generation	Disagree	Nuclear facilities are required by multiple the Code of Federal Regulation (CFR)requirements to maintain configuration control of components. Plant systems and components subject to Cyber Security regulation, either by FERC/NERC or other regulatory agencies are maintained under configuration control due to the CFR programs. Revisiting the classification of assets is not needed to enhance configuration control as on-going design control and configuration management processes are applied to meet the legal requirements implemented by CFR.
5.39	The United Illuminating Co	Disagree	Proposed R3.3 uses the term “such change to the BES” is not clear. The use of the phrase leads to the belief it applies only to 3.2, Did the SDT intends R3.3 to apply to both R3.1 and R.32?Suggest rewording 3.3 to: Update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of reviews required by R3.1 and R3.2.
5.40	Pacific Gas & Electric Company	Disagree	R 3.2 Understand the overall intent of 3.2, however "...any planned change to the portion of the BES..." essentially occurs on a daily basis so unclear on the overall feasibility of this requirement. Suggest 3.2 be more refined than "any planned change to the portion of the BES".
5.41	Reliability & Compliance Group	Disagree	R3.1 is unnecessary with a proscriptive program for identifying BES cyber systems. Therefore, you should only need to review the identification and categorization of your BES cyber systems if there is a planned change to the system or if there is a change to

#	Organization	Yes or No	Question 5 Comment
			the standard's definition of what is or is not a BES cyber system or system component.
5.42	American Electric Power	Disagree	R3.2 and R3.3 are triggered from changes to the BES. Depending upon what constitutes a change to the BES, there could be daily triggering events that would require the review and updates as stated in these two requirements. Will every BES Cyber System (including those not associated with the BES change) need to be reviewed and possibility updated for each and every change to the BES?Furthermore, it appears that it would be possible that a Responsible Entity could be in violation of R3 the Responsible Entity could also be in violation of R1 and/or R2 as well. It appears that R1 and R2 are one-time initial events and that R3 is the on-going requirement replacing those events; however, if that is the intent it is not clear in that regard.
5.43	Consultant	Disagree	R3.2 'any' planned change is probably too broad. Should include addition or removal of BES assets, whether by construction, retirement, purchase, or sale of assets. Some qualification of the changes BES assets that would require review of the identification and categorization of a BES asset would be better. Possible wording "changes to cyber systems or physical protection cyber systems associated with BES assets...", which would appear to be consistent with R23 in CIP-011.Possible "unintended consequence" - requirement R3.2 as stated, and in the suggested changes, requires change control for all BES cyber assets regardless of impact categorization.
5.44	SCE&G	Disagree	R3.2 needs to be clarified regarding "any planned change to the portion of the BES that it owns". What constitutes a change? Is this a Transmission/Generation factility change, operational change, or a cyber systems change, or all three? This has the potential to be interpreted by auditors as needing to be reviewed anytime equipment is replaced.
5.45	Madison Gas and Electric Company	Disagree	R3.2 states " review the identification and categorization of BES Cyber Systems of any planned change to a portion of the BES that it owns". It is unclear how an entity will accomplish a review of a "planned" change. Recommend the "planned" be removed and supplement with "incorporated". R3.2 should read as:"review the identification and categorization of its BES Cyber Systems as a result of any incorporated change to the

#	Organization	Yes or No	Question 5 Comment
			portion of the BES that it owns".
5.46	ERCOT ISO	Disagree	R3.2: Consider: review and document the identification and categorization of its BES Cyber Systems as a result of any planned change to its BES Cyber Systems or BES Cyber System ComponentsR3.3: Recommend that the 45 days be changed to 30 days to align with the changes recommended under FERC Order 706 (i.e., section 651).
5.47	BGE	Disagree	Recommend adding provisions for re-evaluating new systems prior to going live.
5.48	ISO New England Inc	Disagree	Recommend that a local definition of "planned change" is needed. Suggest this definition excludes planned outages or maintenance. Possibly use "modification to Facilitiies" per FAC-009 as a starting point.
5.49	Detroit Edison	Disagree	Remove the "planned change" verbiage in R3.2. Consider changing R3 subrequirement 3.2 to:Each Responsible Entity shall: 3.2 Review the identification and categorization of its BES Cyber Systems as a result of any change to the portion of the BES that it owns that affects the classification of a BES Cyber System or causes the addition or removal of BES Cyber Systems
5.50	Nuclear Energy Institute	Disagree	Requirement 3.2 implies that ALL BES Cyber Systems would need to be reviewed as a result of any planned change to the portion of the BES that it owns. Need to bound this review to only BES cyber systems that are affected by the change. Also, it would be helpful to clarify the term "change" to preclude the triggering of a review for something like a password change.Additionally, the phrase "adequate requirements" in the R3 introductory paragraph should be clarified to "adequate security requirements."
5.51	Southern California Edison Company	Disagree	SCE's concerns regarding Requirement 3.2 are three-fold: (1) Requirement 3.2 appears to require review of all BES cyber systems whenever any change in ownership of any portion of the BES occurs. SCE recommends the drafting team clarify that the review should only occur for systems that are impacted by the ownership change.(2) It is unclear whether Requirement 3.2 adds significant value to the reliability of BES because

#	Organization	Yes or No	Question 5 Comment
			planned changes may not be always approved or implemented as designed and actual changes made would, regardless, have to be documented by R3.3 within 45 calendar days.Finally, the drafting team should make the period after an unplanned change "time-bound" obligating RE's to develop plans to address compliance with CIP standards within a specific timeframe after which R3.2 would become applicable. This approach would be in agreement with the intent of Order 706 which places paramount importance on the reliability of the BES. It is also unclear from this requirement that the timeframe within which a system or component identified in R3 has to adhere to CIP-011. Such a timeframe should be clearly stated within the standard.
5.52	San Diego Gas and Electric Co.	Disagree	SDG&E doesn't necessarily have issues with the 36-month review requirement in R3.1. However, we do have a concern about the 45-day requirement in R3.3 due to the sheer number of BES Cyber Systems that could change. We suggest that this requirement be changed to 90 days so that entities will have adequate time to update appropriate documentation.
5.53	Network & Security Technologies Inc	Disagree	Suggest adding a requirement to review the identification and categorization of its BES Cyber Systems as a result of any planned changes to one or more of its BES Cyber Systems. "Planned changes" include but are not limited to hardware and/or software upgrades adding new functionality, addition of new BES Cyber Systems, retirement or redeployment of existing BES Cyber Systems.
5.54	Allegheny Energy Supply	Disagree	Suggested modification to 3.2:review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates.
5.55	Allegheny Power	Disagree	Suggested modification to 3.2:review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates.
5.56	Dynegy Inc.	Disagree	The 3.3 update should be extended to 6 months. This type of update could be detailed and require more than 45 days.

#	Organization	Yes or No	Question 5 Comment
5.57	APPA Task Force	Disagree	The APPA Task force agrees with some parts of the proposed requirement but we offer the following suggestions:We believe that 3.2 and 3.3 are duplicative and confusing from a monitoring perspective. We also note that there seems to be a gap that does not cover significant changes to BES Cyber Systems. In addition, “ownership” of BES Facilities seems to be the incorrect determining factor, especially since the definition of BES Cyber Systems is focused on operations. It would seem that the focus ought to be on the BES Cyber Systems owned by the System Operator that it uses to operate the BES within its operational scope. We recommend deleting 3.3 and replacing 3.2 with the following:”3.2 Review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it operates. The effective date of any changes to BES Cyber System identification or categorization shall be the in-service date of such change.”Such language would result in the need to plan ahead of time and ensure the documentation is developed, but that it need not be implemented until the in- service date of the new equipment.We also recommend adding a new 3.3 to address significant changes to BES Cyber Systems that may impact identification and categorization, such as:”3.3 Review the identification and categorization of its BES Cyber Systems as a result of change in BES Cyber System configuration or scope. The effective date of associated changes to BES Cyber System identification or categorization shall be the in-service date of such change.”
5.58	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The change management requirements of CIP-011 necessitate lengthening the time to document completed changes to 60 days or more.
5.59	ReymannGroup, Inc.	Disagree	The dynamic and real-time nature of cyber security threats requires a minimum review cycle for identifying and classifying new or changing BES Cyber Systems to 12 months or less as determined by planned or unplanned changes to the BES. Therefore, we recommend revising 3.1 to a 12-month cycle and revising 3.2 to include planned and unplanned changes.

#	Organization	Yes or No	Question 5 Comment
5.60	Bonneville Power Administration	Disagree	The objective of this requirement (“To ensure the application of adequate requirements on its BES Cyber Systems") should be clearly labeled as “Objective of Requirement” and shown as a separate sentence. The Requirement should not include the objective. That would clearly separate the objective from the action(s) that the Responsible Entity must take.3.2 doesn't define the magnitude of "planned change". As defined, it includes routine maintenance such as replacing conductors on a line. A better definition would be "...planned change to the architecture of the portion...". In any event, there must be some way for entities to determine which change triggers a review.
5.61	Manitoba Hydro	Disagree	The requirement needs to include a review of the categorization of the BES Cyber System as a result of a change in the BES Cyber System. Is the intent of Requirement 3.2 to review the identification and categorization of ALL its BES Cyber Systems as a result of ANY planned change to the portion of the BES that it owns? If so, this is excessive and should be limited to BES Cyber Systems impacted by the planned change. If the intent is to limit the review in Requirement 3.2 to the BES Cyber Systems impacted by the change, then the 36 month review in Requirement 3.1 could be continually reset, and an overall review never completed. The period for an overall review should be a fixed interval of every 36 months. Requirement 3.3 language is vague when referring to “such change”. If the intent is to update the documentation in when triggered by events in 3.1 and 3.2, then the language of 3.3 needs to be added to both 3.1 and 3.2. As a result, 3.3 can be deleted. Requirement R3.3 is incomplete or inconsistent as drafted. The first portion of Requirement R 3.3 refers to updating documentation specified in Requirements R1 and R2, which includes a 3 year review, yet the latter portion of Requirement 3.3 specifies that updating must be done within 45 days of a change. It is not clear when updates must be done after a three year review.
5.62	Alberta Electric System Operator	Disagree	The wording of R3.3 implies it is a sub-requirement of R3.2 because of the wording “such change.” Consider revising to “... within 45 calendar days of the completion of such review.”

#	Organization	Yes or No	Question 5 Comment
5.63	EEI	Disagree	There are no boundaries around what constitutes a change to the BES in R3.2 and R3.3. As written, every change to a breaker setting in a BES substation would cause the RE to have to perform a review. The requirement should be rewritten so that only changes which cause a reclassification under Attachment II should be included in this requirement. In addition, the review period should be specified as 45 days from deployment of the change. The change has to be material to the classification criterion in Attachment 2 in order to trigger a review.As noted in EEI's response to Question 3, a Responsible Entity may not need to characterize all the BES Cyber Systems it owns (for example, jointly owned units). EEI suggests the following modification to 3.2:"review the identification and categorization of its BES Cyber Systems as a result of material changes to the portion of the BES that it operates."
5.64	Southern Company	Disagree	There are no boundaries around what constitutes a change to the BES in R3.2 and R3.3. As written, every change to a breaker setting in a BES substation would cause the RE to have to perform a review. The requirement should be rewritten so that only changes which cause a reclassification under Attachment II should be included in this requirement. In addition, the review period should be specified as 45 days from deployment of the change.R.3.2 requires the review of identification and categorization for planned changes. R3.3 requires an update of documentation related to these changes within 45 days of completion. The requirements of R3.2 would be difficult to audit and are better covered under R3.3.
5.65	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
5.66	Independent Electricity System Operator	Disagree	We agree with R3 and its sub-requirements except R3.2. Specifically, we do not agree with the term "the portion of the BES that it owns" since some Responsible Entities do not own any BES facilities. We suggest replacing this term with "the portion of the BES that it owns or operates".

#	Organization	Yes or No	Question 5 Comment
5.67	IRC Standards Review Committee	Disagree	We agree with R3 and its sub-requirements except R3.2. Specifically, we do not agree with the term "the portion of the BES that it owns" since some Responsible Entities do not own any BES facilities but do own Cyber Systems with which they operate the BES. We suggest to replace this term with "the BES Cyber Systems or the portion of the BES that it owns".
5.68	GTC & GSOC	Disagree	We are concerned with requiring an update of all BES Cyber System categorizations whenever planned changes are made to the BES. First, there is a gap here with respect to capturing the changes to the BES Cyber Systems themselves that may affect categorization. Also, this will likely create a complicated compliance tracking scenario for the entity who will be required to track a number of activities to ensure they are completed "within 12 months" of the categorization. We recommend replacing "within 36 months" in R3.1 with "annually" and completely removing both R3.2 & R3.3. This will allow the tracking of compliance activities to occur more on a programmatic basis rather than necessarily on a device by device basis.
5.69	Xcel Energy	Disagree	We believe 60 days is a more appropriate time to allow updating of document under Requirement 3.3. During certain times of the year, (i.e. end of year holidays and financial close out activities) 45 days can be challenging.
5.70	Alliant Energy	Disagree	We believe Article 3.1 is unnecessary and should be deleted. If an entity does an initial assessment and identifies and categorizes its BES Cyber Systems, the only time there would be a change to the listing is if the BES Cyber Systems were modified, which is covered in Articles 3.2 and 3.3. If the SDT determines that Article 3.1 is required, the timeframe should be revised to 60 months to correspond to other summary reviews required by NERC (ie; 5-year analysis of Black-Start capabilities).In Article 3.2 the word "planned" should be replaced with "installed" or "incorporated". There are many modifications planned that never get installed, so it is not reasonable to require all "planned" items to be included.In Article 3.3 the update period should be 90 days not 45, to allow the Registered Entity time to make the necessary changes. 45 days is not

#	Organization	Yes or No	Question 5 Comment
			adequate time to do the updates at the end of a project.
5.71	FirstEnergy Corporation	Disagree	We do not agree with the VRF of High assigned to this requirement and believe a Medium VRF is more appropriate. Violating R3 does not pose the same risk to the BES as violating R1 and R2.As written, 3.2 implies that every change to the BES would trigger a documented review of the cyber system list and becomes a burdensome compliance task. As a compromise we propose that you simplify R3 such that a review/update is required every 18 months.
5.72	We Energies	Disagree	We Energies agrees with EEI suggested modification to 3.2:"review the identification and categorization of its BES Cyber Systems as a result of changes to the portion of the BES that it operates."
5.73	Midwest ISO	Disagree	We request that 3.3 be modified to 60 days rather than 45 days. We believe 45 days will be a challenge for most entities to meet as this effort will likely be incorporated into an entity's broader business continuity efforts.
5.74	Verizon Business	Agree	The requirement should provide guidance relating to when a utility needs to add a new BES system or component and what the timelines are for implementation of the CIP-010, R3 requirements.

6. **CIP-010-1 Attachment I contains a listing and brief description of Functions Essential to Reliable Operation of the Bulk Electric System. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.**

Summary Consideration:

Many entities expressed concerns that Attachment I is part of the standard and includes the use of many undefined terms. Others expressed concerns about the vagueness of many of the terms.

In response to these comments, the SDT has changed the definition of the Reliability Functions to **BES Reliability Operating Services**, and has included these terms in the Glossary. Some modifications have been made to more precisely define the context in many sub-definitions.

#	Organization	Yes or No	Question 6 Comment
6.1	Madison Gas and Electric Company		Recommend eliminating the word "conditions" used in the descriptions of the functions. It's not clear what "conditions" means in the context in which it is used in Attachment I. A function is a set of activities and actions to accomplish an objective or purpose. Such activities and actions may be automatic or manual or a combination of the two and certain tools and infrastructure may be inherently needed to fully execute the functions. In contrast, conditions are states that result from the execution of functions and/or the effects of external, sometimes uncontrollable, factors.Recommend Function section to read:CIP-010-1 - Attachment I Functions Essential to Reliable Operation of the Bulk Electric System The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes. Dynamic Response - Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to a BES activity or action Balancing Load and Generation- Activities and actions for monitoring and controlling generation and load. Controlling Frequency (Real Power)- Activities and actions to control frequency within defined bounds. Controlling Voltage (Reactive Power) - Activities and actions to control voltage within defined bounds. Managing

#	Organization	Yes or No	Question 6 Comment
			Constraints- Activities and actions to maintain operation of BES elements within their design limits and constraints. Monitoring & Control - Activities and actions that provide monitoring and control of BES elements. Restoration of BES- Activities and actions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Situational Awareness - Activities and actions to assess the current, expected, and anticipated state of the BES. Inter-Entity Real-Time Coordination and Communication- Activities and actions for real-time coordination and communication between Responsible Entities' System Operators.
6.2	ISO New England Inc	No	- Recommend "30 minutes" to align with EOP standards- Please provide background for where the 15 minute recommendation came from
6.3	Progress Energy (non-Nuclear)	No	A concern is that depending on how we identify the BES, the 'monitoring & control' function may be associated with many transmission lines that utilize microprocessor relays. Based on the definitions of BES Cyber System Component and the monitoring and control function, this could be interpreted as to being in consideration regardless of whether or not we connect communications to the relay.CIP-010-1 Attachment I - More guidance needed - There needs to be guidance on the definition of 'can have an effect on real-time operation of the BES within 15 minutes'. This leaves too much ambiguity in defining the Cyber Systems that could potentially be covered by the standards and at which level. It could even be interpreted to include systems which may even be beyond the control of the Responsible Entity. The definition needs to provide a bright line of distinction so that systems which have the highest potential of presenting a risk receive the greatest attention to enhanced security - rather than requiring finite resources to be spent filling notebooks with information about low risk Systems/Components.
6.4	Duke Energy	No	Attachment I should not be part of the standard, but should be in a guidance document.
6.5	Kansas City Power & Light	No	Do not agree with the "Inter-Entity Real-Time Coordination and Communication" as the description appears directed toward the devices and systems utilized for verbal communications between Regional Entities and the coordination that occurs as a result

#	Organization	Yes or No	Question 6 Comment
			of those interactions and is outside of the scope of cyber control systems that monitor and control the BES.
6.6	Con Edison of New York	No	One general comment is that CIP-010 should avoid using undefined terms, and use NERC Glossary Terms and cross-references to other Reliability Standards wherever possible.Attachment I is a list of "Functions Essential to Reliable Operation of the BES". The DT has attempted to re-define functions that are already documented in Standards. The definitions should be enhanced to reference the applicable Reliability Standards. o Dynamic Response: The only actions automatically triggered on BES elements are protection systems (see PRC Standards), UFLS systems (see PRC Standards), AGC systems (see BAL Standards), Special Protection Systems and AVR's (see VAR Standards). Everything else is manual operation. It is recommended that the term "Dynamic Response" be removed and replaced with "Automatic Response" and reference the applicable Standards. o "Balancing Load and Generation" and "Controlling Frequency (Real Power)" are the same action. This activity should reference the BAL standards which require BA's to balance generation and tie lines. o "Controlling Voltages (Reactive Power)": This function is addressed by VAR, TOP, and IRO Standards. o "Managing Constraints": If included, this action falls within BAL, INT and TOP standards which should be referenced. o "Monitoring and Control": The definition of the "BES Cyber System" is monitoring and control. Remove this and use the term in the introduction to Attachment I. o "Restoration of BES": This function is addressed by the EOP standards. o "Situational Awareness": Eliminate the "Situational Awareness" function, as this category is too broad and general. o "Inter-Entity Real Time Coordination and Communication": Reference the applicable FERC approved Standards.Also the phrase: "activities, actions, and conditions" at the start of each items is not clear. For example, is an alarm panel an activity, action or condition? Is an HMI computer an activity, action or condition?
6.7	Regulatory Compliance	No	Please see response to question 3.

#	Organization	Yes or No	Question 6 Comment
6.8	Southwestern Power Administration	No	Requiring Responsible Entities to utilize categories which are intended for guidance in identifying BES Cyber Systems, within the reliability standard; and then requiring Entities to be measured by having evidence that those Cyber Systems tie to the functions listed in Attachment I does not further the goal of maintaining reliability and adds complexity and confusion to the process. Attachment I should be converted to a guidance document.
6.9	San Diego Gas and Electric Co.	No	SDG&E would like to request clarification on a definition of the "situational awareness" function. It is too broad for us to effectively determine what assets might be in scope for this requirement. Similarly, we'd also like to request a definition of the term "BES element" in the Monitoring and Control section.SDG&E would also like to request clarification on the "Inter-Entity Real-Time Coordination and Communication" function. Is this meant to cover voice communication between entities or would it also cover electronic data communication between entities such as ICCP data links? We'd suggest that the ICCP links be specifically excluded because it doesn't fit the wording of "real-time coordination or communication between System Operators"
6.10	IRC Standards Review Committee	No	The descriptions for most of the functions in Attachment I are too vague that they cannot serve as a guideline for identifying which components whose Cyber Systems should be included. For example, Dynamic Response" can cover a very wide range of facilities from generator excitation system, stabilizers, governors, AVRs, to SVCs, HVDC controls, switchable shunts, series compensation devices, even under-load tap changers and phase angle regulators, etc. Every one of them has an effect on real-time operations but not all of them, when tempered with, have significant adverse impacts on BES reliability. The list in Attachment I renders almost all facilities to qualify as essential to reliable operation of the BES, but not all of them have any significant impacts on reliability.Attachment II provides a list of facilities to be categorized under various impact levels. We believe this list is more useful in assisting Responsible Entities in identifying facilities whose Cyber Systems are subject to the security requirements. Further, we believe the establishment of this list already had the built-in assumption that

#	Organization	Yes or No	Question 6 Comment
			they perform one or more of the functions listed in Attachment I.
6.11	E.ON U.S.	No	The inclusion within the function "Situational Awareness" of current state of the BES creates an unnecessary overlap with the "Monitoring and Control" function. In addition, this inclusion appears to require tools such as a video wall fall within the scope of CIP standards despite it not being necessary to perform state estimation or operator monitoring of real-time events. E ON U.S. suggests the "Monitoring and Control" function explicitly include real-time monitoring of real-time or current state of the BES and "Situational Awareness" be limited to assessment of the expected and/or anticipated state of the BES. E ON U.S. also notes that in most cases "Restoration of BES" would be greater than 15 minutes The term "effect" in paragraph 1 of Attachment 1 should be defined.
6.12	Nuclear Energy Institute	No	The introductory paragraph should be revised to be more precise. First, "could" should be replaced with "would". Second, it is not clear what "within 15 minutes" constitutes. Leveraging the definition of BES Cyber System, an acceptable opening paragraph would be:The following operating functions are essential to real-time reliable operation of the Bulk Electric System (BES). To define the scope of applicability of CIP Standards, the functions of relevance are only those that would have an effect on real-time operation of the BES within 15 minutes of the BES Cyber Systems that implement them being rendered unavailable, degraded, compromised, or misused.
6.13	Manitoba Hydro	No	The second sentence of Attachment I is unclear. Within 15 minutes of what? Is the reference to "real-time" necessary given the requirement to have an effect on the BES within 15 minutes?
6.14	Midwest ISO	No	We do not believe Attachment I is needed for anything more than a starting point for identifying BES Cyber Systems per Attachment II. Thus, it is not necessary to expand this any further.
6.15	PacifiCorp	Yes	- PacifiCorp agrees with EEI's suggested improvements for Attachment I below:The

#	Organization	Yes or No	Question 6 Comment
			"Situational Awareness" description should be modified as shown below:Situational Awareness -Activities, actions and conditions to assess the current (real-time) state
6.16	Cogeneration Association of California and Energy Producers & Users Coalition	Yes	1. The first paragraph of Attachment 1 to CIP-010 states:". . . the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes." This is a vague statement. Every device connected to the BES will have an effect on real-time operation but some device's effects will be negligible. Clarification is needed on how entities can determine if their assets have a material, non-negligible effect on real-time operation of the BES within 15 minutes when a Cyber System is unavailable, degraded, compromised, or misused.2. In Attachment 1 of CIP-010, Dynamic Response is defined as:"Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition." Examples or guidance on what is covered by Dynamic Response areneeded. For instance, would Automatic Generation Control be considered a Dynamic Response action?3. Attachment 1 of CIP-010 describes Controlling Frequency and Controlling Voltage as functions essential to reliable operation of the Bulk Electric System. Generators provide Real Power (Controlling Frequency) and Reactive Power (Controlling Voltage). However, we are aware of no disturbance to the BES due to loss of Real Power output or Reactive Power output from our generators. Further clarification is required regarding how impact on grid operations should be determined and measured when determining if a function is "essential" to reliable operation.
6.17	Florida Municipal Power Agency	Yes	Although FMPA agrees with the intent of Attachment I, we believe the definitions contained in the attachment can be significantly improved.As discussed in response to Question 3, FMPA recommends using the word "activities" (or other suitable synonym) for the word "function" to avoid confusion with the Functional Model.The description of situational awareness is too ambiguous and can be interpreted in multiple ways. For further clarification, FMPA suggests:"Information processing and presentation within a Control Center to enable operators to assess the current, expected, and anticipated

#	Organization	Yes or No	Question 6 Comment
			state of the BES."FMPA has other recommended changes to help simplify and clarify the definition of terms used:"Dynamic Response - Actions performed by Protection Systems, control systems, and/or BES Cyber Systems which automatically trigger to initiate a response to a BES Disturbance." (Facilities and Elements do not perform any action, protection, control and cyber systems perform the action)Balancing Supply and Load - Activities, actions and conditions for monitoring and controlling supply and Load. (supply is a more encompassing term that includes energy storage, such as batteries, that may not be included in the term "generation", and Load should be capitalized since it is in the Glossary)Managing Constraints - Activities, actions and conditions to maintain operation of the BES within SOLs and IROLs. (by definition, a BES Element is a Facility; hence, if this suggestion is not taken, then BES element ought to be eliminated from the bullet. Additionally, SOLs and IROLs ought to be discussed in this context and those terms subsume Facility design limits)Restoration of BES - Activities, actions and conditions necessary to go from a shutdown condition to an operating condition. (the phrase "delivering electric power without external assistance" adds no value and is not supported by EOP-005).
6.18	Tenaska	Yes	As long as these functions are applied to High and maybe medium BES assets then the cyber system attached to them. Clarification to "monitoring" should be considered to limit applicability.
6.19	FirstEnergy Corporation	Yes	As stated in our response to Question 3 FE believes that adequate critical infrastructure protection and BES reliability can be accomplished without a need for burdensome compliance documentation of functions described in Attachment I. We encourage the team to carefully review its need and consider removing this aspect from the standard. Please see our response to Question 3 for more details.
6.20	Progress Energy - Nuclear Generation	Yes	Attachment 1 needs to clarify that nuclear generating stations defer to the principles of nuclear security first before consideration is given to the bulk electric system.

#	Organization	Yes or No	Question 6 Comment
6.21	Southern Company	Yes	Broad use of Situational Awareness and System Restoration in the BES functions list and definitions cause the scope of the standards to be overly broad, well beyond the point where there is any reliability benefit. Because there are very few programmable devices in any BES facility that do not have some relevance to one of the listed BES functions, the number of devices included in the standard compliance effort will mushroom unmanageably. The large majority of these newly-included devices pose no significant threat to the BES, but the effort of bringing them into compliance will both distract from the efforts to improve security and will reduce reliability by slowing emergency restoration response time.The function list and other parts of the standards should be modified so that only systems which are used directly in regional or larger Situational Awareness efforts or are relevant to the Entity's System Restoration Plan are included.In addition, the definition of "Restoration of the BES" is vague - does "a shutdown condition" refer to the BES being shut down or a BES component is shut down. The wording should be changed to clarify that it is the BES that is in a shutdown condition."have an effect on real-time operation" should be replaced by "have an adverse effect on real-time operation".
6.22	City Utilities of Springfield, Missouri	Yes	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
6.23	LCEC	Yes	Concerned about the 15 minute threshold.All functions should state: Activities, actions OR conditionsSituational awareness: What is the difference between expected and anticipated? This function could reference real-time system operations of the BES instead of the proposed BES Cyber System definition.
6.24	Southwest Power Pool Regional Entity	Yes	Consider modifying the opening statement to read "...can have an effect on real-time operation of the BES within 15 minutes if not mitigated. Clarify that the expectation is to assume the mitigation is not available or fails for the purposes of the BES Cyber System identification."

#	Organization	Yes or No	Question 6 Comment
6.25	Idaho Power Company	Yes	Controlling voltage needs to reference the voltage on the BES, not just voltage in general which could include distribution level. Situational awareness would seem to include a time window beyond the 15 minute criteria especially as it relates to anticipated state of the BES. Inter-entity Real-Time Coordination and Communication is very broad and pulls in communication systems that are required by other reliability standards to be redundant with plans in place to deal with loss of the primary communication channels. Unless all of the redundant systems are compromised, communication can still be accomplished between entities.
6.26	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Yes	Defining metrics is needed somewhere. For instance, requiring Low Impact compliance over Monitoring & Control of a 20 MW cumulative BES system would be outrageous. If real-time operation is interpreted by the auditor as isolation of a faulted line and Dispatch awareness that the line needs to be fixed, what reliability objective is obtained for the BES? Only local level of service is affected.Concerning “without external assistance” for Restoration of BES is not clear. A boundary is not defined so as to know what external help would be. Would this be the Balancing Authority boundary, or the Reliability Coordinator boundary?
6.27	ReliabilityFirst Staff	Yes	Definition of “BES Elements”, What does “external assistance” mean (restoration)?, Sit Awareness: what is “anticipated state”, does communication include functions such as phones or email?
6.28	Puget Sound Energy	Yes	Dynamic Response: This is a poor title, as dynamic response has a specific meaning in Electrical Engineering. The definition is too vague and could be interpreted to include a breaker operation due to a line fault, as this is a “response to a BES condition”. This definition would include the auto switching controls at nearly every distribution substation with a looped transmission line as a BES Cyber System.Controlling Frequency & Controlling Voltage: This definition would include Under Frequency Load Shedding (UFLS) and Under Voltage Load Shedding (UVLS) schemes, which in many cases only drop single distribution banks, effecting 15 MW of load, which has negligible impact on the

#	Organization	Yes or No	Question 6 Comment
			BES.Managing Constraints: This definition would include overcurrent relays, which may only trip a single 115 kV line that serves local load and has negligible impact on the BES.
6.29	EEI	Yes	EEI suggests that the term “Situation Awareness” be deleted because the term is vague and duplicative of the term “Monitoring & Control.” In the alternative, the “Situational Awareness” description should be modified as shown below:Situational Awareness - Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.
6.30	Exelon Corporation	Yes	Generation functions are not explicit in the Attachment I functions, but are embedded/inherent. As a generation owner/operator, Exelon could review the functions of Attachment I and conclude that generation is not a required function, a reasonable approach if considering loss of a single unit or station out of the entire BES. If adopting the proposed CIP-010 approach, we recommend explicit inclusion of generation as necessary to ensure the Adequate Level of Reliability of the BES.
6.31	The Empire District Electric Company	Yes	I disagree with keeping Attachment I in the standard. The conceptual discussion of functions only adds redundancy, complexity and confusion. The suggested changes to the definition of BES Cyber System and BES Control Center should be enough guidance to identify what is in scope. Therefore, I recommend that the SDT either eliminate Attachment I or convert it to a reference/guidance document supporting the standard
6.32	Consultant	Yes	I think the "15 minute" criteria needs additional clarification. As stated, "an effect on real-time operation of the BES within 15 minutes." is very broad. Suggest limiting to "adverse effect". Also could include some terminology about "adverse effect preventing or limiting the capability of BES assets to perform the listed functions."Suggest numbering the defined functions to allow easier cross-reference to this attachment.
6.33	Alliant Energy	Yes	In paragraph 1 the phrase “that can have an effect on real-time operation” needs to be

#	Organization	Yes or No	Question 6 Comment
			clarified. We believe it should be tied to and IROL, SOL, or degradation of the reliability of the BES. As written it is undefined and too ambiguous.In the item listed "Monitoring & Control" we do not believe monitoring should be included as listed it is too ambiguous and could be interpreted to include every meter, instrument transformer, etc, even if it is not needed for protection of the BES.
6.34	Luminant	Yes	Is it possible to have a real time impact (15 minute time horizon) related to Situational Awareness for Generation? If not it should be removed. At most it should be scoped to BA, RC,TOP and then only to a subset of data.The definitions in Attachment I are very broad. Could the SDT include examples or a reference document that provides more details for the functions in Attachment I?
6.35	Detroit Edison	Yes	It is not clear how the list in attachment 2 was created. Consider leveraging other NERC documents such as the Definition of Adequate Level of Reliability located at http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf.
6.36	Reliability & Compliance Group	Yes	It needs to be more clearly defined what it means to have an effect on real-time operation of the BES. There are many things that can have an effect on the BES that occur even during normal operations. Recommend that the effect be defined as a reduction in the stability of the BES and that level of reduction needs to have a quantifiable measure.
6.37	US Army Corps of Engineers, Omaha Distirc	Yes	It seemes clear from the workshop that the committee intends for protective relay systems to be include for consideration. That was not clear prior to the workshop. They appear to fall under the category of Dynamic Response. Suggest strengthening the definition and include the term "protective relay."
6.38	US Bureau of Reclamation	Yes	It would be helpful to provide a example list of some of the elements which provide the related functions. Further, the unclear definition for "could have an effect on real-time operation..." as used in the opening of Attachment I, needs to be clarified/quanitized or defined. Almost any of these functions (and many more), at any facility - no matter the

#	Organization	Yes or No	Question 6 Comment
			size - could have an effect. The effect needs to be characterized as more than trivial to be deemed essential to reliable BES operation. Rather that attempt to define Restoration of the BES in the Attachment, would it be better to refer to other Standards?
6.39	Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
6.40	MidAmerican Energy Company	Yes	MidAmerican Energy agrees with EEI's suggested improvements below:The "Situational Awareness" description should be modified as shown below:Situational Awareness - Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.Suggest the following addition for Attachment I:Plant cyber systems or cyber components that do not provide or support BES Cyber System (CIP-010 definition) functions (CIP-010, Attachment I) and which logically are external to the electronic boundary (ESP) protecting a BES Cyber System are excluded from the CIP-011 requirements. Examples of excluded components and systems are those that 1) support balance-of-plant functions and operations that cannot directly result in the loss of generating capacity within 15 minutes, and 2) are logically external to the electronic boundary (ESP) protecting a BES Cyber System.
6.41	Oncor Electric Delivery LLC	Yes	Need more clarity on the "15-minute" criteria. Is this ADVERSE effect? Is this RESTORATIVE effect?
6.42	USACE HQ	Yes	Please read answer to question 3.
6.43	BGE	Yes	Provide examples or definitions of actions, activities and automatically triggered.Add the words "to the BES" after "delivering electrical power" in the definition of Restoration of BES to clarify. Further define the Inter-Entity Real Time Coordination and Communication Function (currently implicates, phone system, harmony, email, PJM all

#	Organization	Yes or No	Question 6 Comment
			call system, 800 MHz devices used to communicate to field personnel and notifind)
6.44	SCE&G	Yes	Remove the 15 minute timeframe.
6.45	Southern California Edison Company	Yes	SCE's concerns with the proposed criteria are two-fold. First, it is unclear whether the term "effect" and "disturbance" refer to the same event. Thus, SCE asks the Standards Drafting Team to clarify. As the criterion is currently written, Attachment I states, "To define the scope of applicability of CIP Standards, the functions of relevance are only those that can have an effect on real-time operation of the BES within 15 minutes." However, the definition of BES cyber system in this standard states, "One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES." If "effect" means "disturbance to the BES, restricted control and operation of the BES, or affecting situational awareness of the BES", then the definitions are consistent. This being said, it is not clear that these have the same meaning. An extreme definition of "effect real-time operation" could be virtually anything whether the impact on operations will be significant or not.Additionally, SCE recommends treating control and monitoring as separate functions. Systems that are only capable of monitoring BES elements should be treated differently from systems that are able to perform control functions. SCE suggests the drafting team add an additional function that is based on "actual device capability" rather than "how it has been implemented" by a particular registered entity. For instance, HMI's providing electronic output have a different real-time impact on BES reliability than HMI's designed as I/O devices. The task of reviewing data on a "view only" capable system resulting in human action on another system that could potentially cause BES reliability issues is a distinctly different function than the task of initiating actions. In this case, the monitoring system and the control system are both "real-time" but with very different BES impact potential.
6.46	Constellation Energy	Yes	See answer to Question 3.

#	Organization	Yes or No	Question 6 Comment
	Control and Dispatch, LLC		
6.47	Constellation Energy Commodities Group Inc.	Yes	See answer to Question 3.Provide examples or definitions of “actions”, “activities” and “automatically triggered” as provided in Attachment I.Add the words “to the BES” after “delivering electrical power” in the definition of Restoration of BES to clarify. Further define the Inter-Entity Real Time Coordination and Communication Function (currently implicates, phone system, harmony, email, PJM all call system, 800 MHz devices used to communicate to field personnel and notifying).Please define the industry use for the term Generation Management System (“GMS”). We believe there are two categories of GMS, Regulated and non-Regulated Utilities since they could be use differently or have different functionality.
6.48	MWDSC	Yes	See comments for question 3 above.
6.49	Wolverine Power	Yes	See comments listed for 1.a
6.50	BCTC	Yes	See previous response 0n CIP-010-1-R1
6.51	Dynegy Inc.	Yes	Show examples of how the identification and categorization and tie-in to Attachment 1 would work.
6.52	Constellation Power Source Generation	Yes	Some of the terms are ambiguous. What is meant by monitoring and control? As written, it is an AND statement, meaning that a BES Cyber System would have to do both monitoring AND control to be labeled a BES Cyber System. What about electronic metering at a plant? That provides monitoring, but not control. So is it excluded?Situational Awareness should be clarified. A suggestion would have the following statement attached to the current definition: “and cause an action without further analysis.” This would exclude metering that, if rendered unavailable, would not be detrimental to the BES as phone communication would be used in the event of metering errors.

#	Organization	Yes or No	Question 6 Comment
6.53	Platte River Power Authority	Yes	Suggest removing “Inter-Entity Real-Time Coordination and Communication” until there is a mechanism to define a single BES Cyber System that includes BES Cyber System Components from multiple Entities. The mechanism should include documentation of coordination with implementing the CIP standards for the BES Cyber System.
6.54	SPS Consulting Group Inc.	Yes	Suggestion number one is to get rid of the list, as previously stated. Failing that my other question is about Dynamic Response. I assume this refers to things like UFLS, UVLS and runbacks initiated by SPS. Also assume this does not include things like AGC, AVR, and governor response from generators since these actions are not triggered by a single element or control device, or a combination of devices, but rather are initiated by operating condition fluctuations. Is that true?
6.55	Dairyland Power Cooperative	Yes	Systems used to communicate between entities are not mentioned, yet many of these are critical to the operation of the BES. Imagine the impact to the BES of an ISO/RTO without ICCP communications. How can these systems be ignored?
6.56	Allegheny Energy Supply	Yes	The “Situational Awareness” description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.Suggest that the definitions for "Dynamic Response" and "Balancing Load and Generation" be more specific.
6.57	Allegheny Power	Yes	The “Situational Awareness” description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.

#	Organization	Yes or No	Question 6 Comment
6.58	APPA Task Force	Yes	The APPA Task force agrees with the intent of Attachment I. We believe, however, the definitions contained in the attachment can be substantially refined and improved.As discussed in response to Question 3, we recommend using the word “activities” (or other suitable synonym) for the word “function” to avoid confusion with the Functional Model.The description of situational awareness is too ambiguous and can be interpreted in multiple ways. For further clarification, We suggest:Situational Awareness - Information processing and presentation within a Control Center to enable operators to assess the current, expected, and anticipated state of the BES.Other recommended changes to help simplify and clarify the definition of terms used:Facilities and Elements do not perform any action, protection, or control; rather cyber systems perform the action. Therefore we propose:Dynamic Response - Actions performed by Protection Systems, control systems, and/or BES Cyber Systems which automatically trigger to initiate a response to a BES Disturbance. Supply is a more encompassing term that includes energy storage, such as batteries, that may not be included in the term “generation.” Therefore we propose:Balancing Supply and Load - Activities, actions and conditions for monitoring and controlling supply and load. SOLs and IROLs should be discussed in this context. If this suggestion is not taken, then “BES element” should be eliminated from the definition. Therefore we propose:Managing Constraints - Activities, actions and conditions to maintain operation of the BES within SOLs and IROLs. The phrase “delivering electric power without external assistance” is not supported by EOP-005 and should be removed from this definition. Therefore we propose:Restoration of BES - Activities, actions and conditions necessary to go from a shutdown condition to an operating condition. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES and should therefore be removed from the Monitoring and Control function. Therefore we propose:Control - Activities, actions and conditions that provide control of BES elements.
6.59	Arizona Public Service Company	Yes	The APS review team had the following comment: The document heading is “Function Essential to Reliable Operation of the Bulk Electric System.” Typically restoration of BES

#	Organization	Yes or No	Question 6 Comment
			is a completely different activity than the normal or emergency operation of the BES. The document includes restoration which is typically not essential to the reliable operation of the BES. This is not a contradiction but the operation is being defined more broadly than typical. This broad function description can create ambiguity.
6.60	Independent Electricity System Operator	Yes	The descriptions for most of the functions are too vague that they cannot serve as a guideline to identifying those components whose Cyber Systems should be included. For example, Dynamic Response" can cover a very wide range of facilities from generator excitation system, stabilizers, governors, AVRs, to SVCs, HVDC controls, switchable shunts, series compensation devices, even under-load tap changers and phase angle regulators, etc. Every one of them has an effect on real-time operations but not all of them, when tampered with, have significant adverse impacts on BES reliability. The list in Attachment I renders almost all facilities to qualify as essential to reliable operation of the BES, but not all of them have any significant impacts on reliability.Attachment II provides a list of facilities to be categorized under various impact levels. We believe this list is more useful in assisting Responsible Entities in identifying facilities whose Cyber Systems are subject to the security requirements. Further, we believe the establishment of this list already had the built-in assumption that they perform one or more of the functions listed in Attachment I.We suggest Attachment I be eliminated.
6.61	Entergy	Yes	The Functions as identified in Attachment I are far too general in nature and thereby leave too much latitude in interpretation in audit, i.e., creates a risk that if the Responsible Entity excludes a system(s) from scope and the auditor disagrees, this could be a very significant adverse finding. Entergy recommends that general Function descriptors be augmented with specific examples of applications that execute the stated functions 'essential to reliable operation of the BES', e.g., ACE, AGC, state estimator, etc., to help avoid as this dilemma to the extent foreseeable.
6.62	NextEra Energy Corporate Compliance	Yes	The standard should clarify those functions and provide examples specific to Generation, Transmission and Control Center Facilities. These clarifications, we believe, should be contained in the body of the standard as opposed to a reference attachment.

#	Organization	Yes or No	Question 6 Comment
			Attachments should be used to add specific examples or propose exclusions.With respect to the Inter-Entity real time coordination and communication function, the standard should specifically exclude voice communications systems due to the fact that they are covered under separate standards (i.e. COM Standards)
6.63	American Electric Power	Yes	The terms "Dynamic Response" appears to be a very broad function. Is it the intent that this would include all devices such as relays?The "monitoring" portion of function "Monitoring & Control" is too ambiguous. We would propose using the following: "Control - Activities, actions and conditions that provide control of BES elements."In addition, "Situational Awareness" is ambiguous; systems that are not needed for operating the BES, but provide information would be in scope. This definition appears to include items such as all meters, instruments, and transducers.
6.64	Dominion Resources Services, Inc.	Yes	There is overlap among the many functions listed. The list can be reduced to only Monitoring & Control with many of the others listed as examples of this function. As examples; Balancing Load and Generation and Controlling Frequency (Real Power) are essentially the same. Frequency is a direct result of the balance between supply (generation) and demand (load). It is redundant to list both, and doubly redundant since both are covered by Monitoring & Control. Monitoring & Control touches or covers most of the other listed functions. Any portion of Dynamic Response, Controlling Frequency (Real Power), Controlling Voltage (Reactive Power), and Managing Constraints not captured in the Monitoring & Control function should be identified and listed separately, but not those entire functions. Also, some of the definitions are too broad and encompass functions that are not required for the reliability of the BES.Facilities must have ratings per FAC-008 and must be operated within those ratings in other reliability standards. Please refer to “ratings” rather than “design limits and constraints.”Dominion requests that the functions be reduced to: Monitoring & Control - Activities, actions, or conditions that provide real-time operation and control to maintain BES elements within their ratings. Restoration of BES (as defined).Situational Awareness - Activities, actions, or conditions required by the BA, RC, or TOP for real-time operational decision-making associated with the BES.Inter-Entity Real-Time Coordination

#	Organization	Yes or No	Question 6 Comment
			and Communication (as defined).
6.65	Pepco Holdings, Inc. - Affiliates	Yes	We agree with EEI's comments.
6.66	We Energies	Yes	We Energies agrees with EEI comments. The "Situational Awareness" description should be modified as shown below:Situational Awareness -Activities, actions and conditions essential for to assessing the current (real-time) state of the BES.It is not appropriate to treat any or every item that provides some level of information about the status of the BES as high level impact. Certain components are simply informational and not required for real time operations.We Energies agrees with EEI Suggest the following addition for Attachment I:Plant cyber systems or cyber components that do not provide or support BES Cyber System (CIP-010 definition) functions (CIP-010, Attachment I) and which logically are external to the electronic boundary (ESP) protecting a BES Cyber System are excluded from the CIP-011 requirements. Examples of excluded components and systems are those that 1) support balance-of-plant functions and operations that cannot directly result in the loss of generating capacity within 15 minutes, and 2) are logically external to the electronic boundary (ESP) protecting a BES Cyber System. Additionally, We Energies does not understand the inclusion of "Real "Power" and "Reactive Power" in the context of the functions "Controlling Frequency" and "Controlling Voltage" respectively. It is suggested that these qualifiers be eliminated.
6.67	Bonneville Power Administration	Yes	We find the guidance on Attachment I confusing. The statement "The following operation functions are essential to real-time reliable Operation of the Bulk Electric System" makes the explicit statement that all the functions listed below are essential to real-time operation; and the second sentence doesn't do a good job of clarifying that it is only those BES Cyber Systems for which the loss of the functions listed below (Dynamic Response, Balancing Load and Generation, Situational Awareness, etc.) can have an effect on real-time operations of the BES within 15 minutes.For example, the loss of a cyber system used for situation awareness of lightning strikes would not have an effect on real-time control and operations of the BES within 15 minutes. As such, it is NOT a

#	Organization	Yes or No	Question 6 Comment
			BES Cyber System.It would be helpful if this statement in Attachment I and the definition of BES Cyber System were more consistent with each other."Situational Awareness" is too broad. Refer to comments in Question 1.b.
6.68	American Transmission Company	Yes	We propose to remove “monitoring” from the Monitoring and Control function. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES.We would propose using the following:Control - Activities, actions and conditions that provide control of BES elements.
6.69	MRO's NERC Standards Review Subcommittee	Yes	We propose to remove “monitoring” from the Monitoring and Control function. As written, the term “monitoring” is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES.We would propose using the following:Control - Activities, actions and conditions that provide control of BES elements.
6.70	WECC	Yes	While scoping the CIP standards to only cover functions within a 15-minute event time frame is appropriate for generation, transmission, and other operations it is not appropriate for Reliability Coordination functions such as situational awareness. There are many cases of critical systems to support a reliability coordination function that do not fall within a 15 minute time horizon such as next day studies, coordinated outages, and contingency planning. Suggest that the SDT redefine functions for situational awareness and communication between entities to not be restricted to a 15 minute time period.The opening paragraph again refers to a 15-minute time period to be used in the identification of BES Cyber Systems. It appears that an effort is being made to restrict applicability of this standard to real-time systems. Section 215 of the Federal Power Act does not include such a restriction; therefore, this should be removed from the standard. Any cyber system that could affect the reliability of the bulk electric system, regardless of timeframe, should be in-scope.Dynamic ResponseThe second sentence is poorly worded and does not appear to add anything. This language should be clear and concise.Restoration of BESThere are a significant number of restoration plans at the

#	Organization	Yes or No	Question 6 Comment
			Balancing Area and Transmission Operator level that hinge on external assistance. In many cases these areas play a significant role in delivering power across the transmission system during restoration, but do require external assistance. As drafted, the functional characterization for restoration of the BES, may fail to identify systems critical to system restoration and is seemingly inconsistent with Attachment II, specifically Item 1.6.
6.71	Ameren	Yes	Would change the second sentence defining the scope to read "To define the scope of applicability of CIP Standards, the below functions are relevant only if they can have an effect on real-time operation of the BES within 15 minutes.Would suggest to impose limits on the definitions for example Controlling Voltage (Reactive Power) is partially dependent on hydrogen pressure for hydrogen cooled generators. We would also suggest adding the word "grid" in front of voltage.Change the first sentence of Dynamic Response to read "Actions performed by BES elements or Facilities which are automatically triggered to initiate a response to mitigate the impact to a BES condition". Is it the SDT intent to implement physical and cyber security of any tertiary systems for example, Controlling Frequency (Real Power) is also dependent upon coal mills providing enough fuel to the boiler, do these systems also need to be secured?The "Controlling Frequency" section needs some clarification. Governor controls on all generating units have built mechanisms whether mechnical or electronic that act to control or balance frequency during a disturbance. The current definition would lead to inclusion of all generating units regardless of any other factor. â€,The last section on communication needs to be clarified to explicitly address voice communication vs. data communication and the expectations of both.
6.72	Verizon Business	Yes	The criteria should include major systems needed for the essential operation of such systems as control centers. For example, Heating, Ventilation and Air Conditioning (HVAC) systems are essential to the operation of a control center. The failure of the HVAC could lead to shutdown of the control center within the 15 minute time frame.

7. CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

Summary Consideration:

The summary of responses to Question 7 was previously posted on the NERC website prior to the posting of Version 4 of the CIP-002 through CIP-009 standards.

#	Organization	Yes or No	Question 7 Comment
7.1	Platte River Power Authority		1.1 is confusing. Consider revising: For the preceding 12 months did the Generation Facility's net Real Power capability (rated net) exceeds the largest value of either the Contingency Reserve or the Reserve Sharing Group's total reserve sharing obligation. In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW. 2.7. "switching stations operated at 200kV or above" should read "switching stations operated between 200kV and 299kV"
7.2	National Rural Electric Cooperative Association (NRECA)		In 1.1, "must run" must be more clearly defined and there needs to be language to make clear how Generation Facilities are labeled "must run" -- i.e., who determines the "must run" status? In 1.5 and other places in this document, the term Transmission lines is used. What does "lines" mean? One wire? One three-phase circuit? One single phase of a three phase circuit? Please make this clear so there is no confusion for registered entities when determining High, Medium or Low. In 1.10, please provide an explanation of what "impact" and "local area" means in the phrase "have impact beyond the local area." Add language to 1.10 as needed to make

#	Organization	Yes or No	Question 7 Comment
			this more clear.
7.3	Emerson Process Management		It is only uncertain how the criteria of 2000MW and 1000MW were chosen for generation facilities.
7.4	Arizona Public Service Company		These criteria are closely related to the definition of a BES Cyber System and the feedback for question #2. If the intent is to categorize the majority of BES Cyber Systems into the Low, Medium and High Impact Categories, with the current timeline specified in the definition of a BES Cyber System, it may lead Entities to exclude from Impact Categorization (by the Definition) Cyber System Components that the drafting team did not intend. A preferred approach may be to eliminate the time windows from the definition, causing all BES Cyber Systems to be inventoried, and enhancing the Impact Categories with additional time window criteria. For example, a High category may be further refined by specifying an impact window of 0-15 minutes, a Medium of 16-240 minutes, a Low of 241-1440 minutes (24 hours), etc. Additionally, a further Impact Category of 'None' may be beneficial if the 15-minute time windows is removed from the definition. This would allow a floor to be utilized in the Impact Categorization of 'Low' so that it would not result in unintended consequences of including undesired BES Cyber System Components in a category with Standard applicability. Further comments regarding the (as-of-yet undefined) implementation schedule include concerns that a long implementation schedule or different implementation schedules for High, Medium and Low both raise the risk of confusion as well as the risk or FERC disapproval. An alternate method, in conjunction with the definition and Impact Category adjustments mentioned, of creating a phased implementation schedule, by time period (12 months, 24 months, 36 months, for example) would allow the applicable standards to increase over time for the lower categories. This would also allow for some Standards to be applied earlier than other Standards in the same Impact Category.
7.5	ISO New England Inc	No	"Must run" in 1.3 and 2.3 is a phase should not be used, even if quotations are around it, because it is a regulatory mechanism, used in some areas of the country, to ensure generators receive adequate payments. Other generators - that are equally important

#	Organization	Yes or No	Question 7 Comment
			to grid operation - may not have reliability must-run agreements. In short, these agreements are established simply as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators are impactive on the bulk electric system. If the Standard Drafting Team insists on using the term, it must, at a minimum, define what it means by this phrase.
7.6	Madison Gas and Electric Company	No	1.3 and 2.3 utilize the words “must run”. Must run is used in many markets whereby a GO may designate a unit to be online outside the need for reliable operations of the BES. Since “must run” is not defined, it is recommend that the SDT remove the term “must run”.
7.7	Progress Energy (non-Nuclear)	No	All T/D substation capacitor banks that provide system reactive support are controlled through a capacitor bank control program residing on the substation gateway device. However the DSCADA master may be included in 1.2 (more than 1000 MVAR). 2.4 will bring many T/T substations into consideration with the four or more lines >200kV. Also see comment 4. Attachment II defines "Each Cyber System that can affect operations for..." as it relates to Impact Rating on BES. For new combined cycle facilities which will include diverter dampers to allow simple cycle operation can we designate separate Cyber systems for simple cycle operation (approximately 70% of total plant output) and combined cycle operation (approximately 30% of total plant output). Potentially that would define each system as a "Low " impact versus a combined Medium to High. The plants are being designed to go from combined cycle to simple cycle operation in less than 15 minutes. We will need to know whether this designation is allowed and then design the cyber system(s) architectures appropriately.
7.8	Consultant	No	Attachment II - Section 1.1 & 1.2 To avoid confusion, suggest consistent wording in the parenthetical phrases following the words "singularly or in combination" in these sections.

#	Organization	Yes or No	Question 7 Comment
			Section 1.2 - Similar to section 1.1, should there be a 12 month component to the Reactive Power criteria in addition to the 1,000 MVAR. Section 1.3 & 2.3 - The term "pre-designated" doesn't make sense. A facility is not in the "must run" status unless it is "designated". Additionally, the statement has "must run" units both "designated" and "assigned", and semantically these are two different conditions. Section 1.3 & 2.3 - Further, the reliability "must run" status is an economic and contractual condition rather than a BES operational condition. It would seem that the plants that would be designated as reliability "must run" should have a BES operational or reliability criteria, independent of their "must run" status, which should be the criteria used to include or exclude these facilities. Section 1.6 - suggest including the title of EOP-005 in the statement as a complete reference citation. Section 1.9 - suggest including the title of NUC-001 in the statement as a complete reference citation. Section 1.10 - suggest clarifying which entity makes the determination that a RAS has "impact beyond the local area." - RAS Owner, RAS Operator, or appropriate regional entity. Section 1.11 (& throughout CIP-011) - BES Elements, BES elements, and elements are used throughout this standard. It is not clear if all are intended to be the glossary definition of 'Elements', or if 'BES elements' or 'BES Elements' are new definitions or incorrect application of the glossary term 'Elements'. Please clarify the usage. Sections 1.8, 1.13, 2.5 - These sections include the words "singularly or in combination" without a subsequent parenthetical qualifier. Suggest consistency with sections 1.1 & 1.2 as discussed above. Section 2.1 - See comments on sections 1.1 and 1.2 regarding consistency of parenthetical statement.

#	Organization	Yes or No	Question 7 Comment
			Section 1.1, 1.3, 1.4, 1.5, 1.7, 2.1, etc. - Multiple sections use the terms Generation Facilities or Transmission Facilities with capitalization that should indicate a defined term, either by this standard or in the current glossary. These terms are not defined in the current glossary. Suggest consistency of using defined terms throughout the standard. Section 2.1 - The criteria in this section are not parallel to the criteria in section 1.1 with a 'downsized' value. The term "most current and prior to most current rated" is not defined, or included in the glossary. Suggest clarifying this section, and defining or referencing the terminology.
7.9	E.ON U.S.	No	CIP-010-1 Attachment II - Impact Categorization of BES Cyber Systems currently lists 14 “High Impact Ratings” of the categorization of the BES Cyber Systems. E ON U.S. proposes that only Control Centers and Backup Control Centers fall into the High Impact Rating category. All other points listed in the High Impact Rating category should be moved to the Medium Impact Rating category, and all points currently listed in the Medium Impact Rating category should be moved to the Low Impact Rating category. More generally, “reliable operation” of the interconnected BES is defined in Section 215(a)(4) as:” . . . operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements.” Attachment II’s low impact category appears completely untethered to the statutory definition of reliable operation of the bulk power system. Attachment II also appears to introduce an ill-defined set of multiple contingencies or sequence of events that needs more definition and boundaries to be of any practical use and to provide a reasonable means for compliance cost quantification.
7.10	Kansas City Power & Light	No	Do not agree with several of the items listed in Attachment II.

#	Organization	Yes or No	Question 7 Comment
			Items 1.7 & 1.8 are too broad. There are any number of combinations of transmission facilities that can be removed from service such that the undesirable effect of exceeding an IROL limit or the loss or reduction of generation would occur. Recommend their removal as the remaining items left in Attachment II are sufficient to capture the HIGH impact areas. Item 1.10 regarding SPS is too broad. SPS systems are in place for a number of different reasons, including the protection of facilities from damage. The SPS that should be considered here are only the SPS that are intended to prevent cascading, uncontrolled separation, or instability. Item 1.14 is too broad and would include facilities that are unnecessary. Recommend tying Control Centers in where facilities are identified in 1.5. Recommend the following language for consideration: Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations for transmission facilities identified by 1.5.
7.11	FirstEnergy Corporation	No	FE suggests that item 1.5 be removed such that it is effectively reclassified as a medium impact and covered by item 2.4. Within the High Impact category, items 1.6, 1.7 and 1.8 appropriately cover those situations where Transmission Facilities should rise to a High Impact level. Consider removing item 1.9. This delves into a nuclear plant safety concern that is covered by the NUC-001 standard and not directly associated with BES reliability. If in item 1.1 a 2000MW level adequately depicts a High Impact generation facility hurdle then transmission facilities associated with a 900MW nuclear plant should not be deemed High Impact for BES reliability. In item 1.10 the term “local area” is vague and open to interpretation. Its suggested to simplify such that all SPS and RAS systems would be treated as High Impact. If the intent is to exclude SPS or RAS associated with limiting generation output under contingency loss of certain Transmission Facilities then consider a separate Medium Impact SPS or RAS describing those instances and rewrite 1.10 to say “Special Protection Schemes,

#	Organization	Yes or No	Question 7 Comment
			Remedial Action Schemes (RAS) or automated switching of BES elements not include in Section 2, item 2.x" However, the preference is to keep it simple and just treat all SPS and RAS items as High Impact. Suggest adding thresholds below which no measures need to be taken. The low impact rating as written could require significant effort for negligible security and reliability improvement.
7.12	National Grid	No	In lieu of the BES NOPR and the exemption process currently proposed, if facilities above 100 kV are exempted by NERC and FERC, will those facilities automatically be exempted from CIP standards? Currently, as per the standards, all the BES systems which are not categorized high impact or medium impact will be defaulted to LOW IMPACT category regardless of how the facility is impacting the Bulk power system. There are facilities >100kV having very localized impact and minimal impact to the reliability of the BES system for which entities will request for exemption. National Grid requests the SDT to clarify this issue. National Grid recommends a tabular format similar to the tables in CIP-011-1 with various criteria listed under Low Impact, Medium Impact, and High Impact. This will help in understanding the key differences among the three categories efficiently."Must run" in 1.3 and 2.3 is a phase should not be used, even if quotations are around it, because it is a regulatory mechanism, used in some areas of the country, to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must-run agreements. In short, these agreements are established simply as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators are impactive on the bulk electric system. If the Standard Drafting Team insists on using the term, it must, at a minimum, define what it means by this phrase.
7.13	American Electric Power	No	Overall we like the concept of these gradients, but need more time to fully ascertain the validity of the breakpoints. It is uncertain what engineering analysis drove these specific categorization levels. We assume that there could be a significant difference from region

#	Organization	Yes or No	Question 7 Comment
			to region, and the SDT should consider regional impacts for the categorization.
7.14	Regulatory Compliance	No	Qualifier should include capacity factors averaged over the last five years - otherwise it will require some large plants that are only on-line several days a year to remediate to the "High Impact" category
7.15	Manitoba Hydro	No	Regarding criterion 1.1, the phrase “with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW” is difficult to understand. For some utilities, the required reserve obligations could be a small value which would not compare very well to the proposed 2000 MW limit for utilities with NO reserve obligations (such as small utilities). A related minimum value for utilities with reserve obligations should be provided, or the greater value of the required reserve obligations and 2000 MW should be used .Regarding criteria 1.5 and 2.4, clarify the requirements through the appropriate use of colons, semi-colons and numbers. It is not clear as drafted whether phrase “with four or more transmission lines” applies to Texas and Quebec.
7.16	Seattle City Light	No	see prior comments
7.17	Indeck Energy Services, Inc	No	The system of 3 categories oversimplifies the BES. 1) The grouping of, for example, all generators of capacity less than 1,000 MW (except for special cases like Must Run units) as LOW needs to be further subdivided. The categorization ignores the Functions in Attachment I. Not all generators have the same impact on the BES ALR for all functions. Different types of generators have different effects on the BES ALR. This isn’t to say that all generators should not be categorized, but not all require the same LOW level of requirements. Choosing only 3 categories was highly arbitrary. The LOW category should be subdivided into 3 or more groups reflecting the relative impact on BES ALR that was used to differentiate the HIGH and MEDIUM groups. 2) Additionally, the standards ignore the fact that access to BES cyber facilities can be

#	Organization	Yes or No	Question 7 Comment
			controlled at either end of a communications path. If it is adequately controlled at one end, then controlling the other end or the middle is less important, if not unimportant. For example, an RTU at a small generator that is a window to the BES cyber facilities at the control center is a bigger risk for BES ALR at the control center than it is at the generator. Any effect on the generator may be insignificant, whereas, access to the control center could be critical. Applying controls at the control center takes away the need to control all of the insignificant RTU's, but not the ones affecting other parts of the BES. 3) Nowhere in the categorization process is the potential impact on BES ALR assessed by Function. Attachment II makes arbitrary categories that may be appropriate for the HIGH and MEDIUM categories, but has not been done for the remainder that are lumped in the LOW category. The concept of impact to the BES ALR is missing from the categorization process. The impact on the BES ALR of, for example a 999 MW generator versus a 499 MW generator versus a 299 MW generator are very different and different by Function as well. The impact on the BES ALR should be assessed for all facilities in the LOW category to differentiate them. All of the facilities should be categorized as to the impact on the BES ALR by function. [suggestion] There should be 5 categories: VERY HIGH, HIGH, MEDIUM, LOW and VERY LOW based upon the relative impact on the BES ALR, with various combinations of facility types and functions from Attachment I.
7.18	Reliability & Compliance Group	No	These criteria do now however, exclude many systems that were previously identified as CCA's. However they also include many systems that registered entities eliminated using the RBAM.
7.19	BCTC	No	This looked very thorough. Great job!
7.20	Xcel Energy	No	While the draft provides guidance in Attachment II as to which BES elements are classified as High, Medium, and Low impact, no criteria is provided for why each element was assigned into the specific impact category. The decision to place each element into

#	Organization	Yes or No	Question 7 Comment
			a category is not based on any identified objective criteria. The SDT should publish the criteria used to place each item under the assigned category.
7.21	Independent Electricity System Operator	Yes	(1) We support explicitly including Restoration of BES as a critical function. However, in the proposed standard it is limited to blackstart generation and transmission subsystem cranking paths (impact level H, items 1.4 and 1.6 in Attachment II). The impact criteria do not include a requirement to protect sufficient generation capacity to allow restoration to proceed to a point of relative assurance of stability and resiliency (not necessarily all load served). With these criteria, in Ontario we would drop 6 generating stations (a total of over 3000 MW capacity) from a High impact (current Critical Assets) to a Low impact category. We suggest to add a requirement in the High category for generation essential to facilitate restoration as determined by the RC. (2) 1.3 “Generator pre-designated as must run”: In some developed markets, must run generators change from time to time and often are not determined (designated) until week/day ahead of real time. We do not believe facilities of this dynamic nature should be included. If we want to include generators having a significant impact on reliability in this category, we need only to say: “Generation Facilities that have Wide Area reliability impacts when removed from service”. (3) 1.7: Violating IROL does not result in instability, uncontrolled separation or cascading. In everyday operations, IROLs are exceeded from time to time due to changing system conditions and external impacts. For so long as such exceedances are corrected within Tv, the BES is deemed to be reliable. We suggest the first part of this category be removed. Keeping the second part “Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading would suffice. (4) 1.13: BA does not operates transmission facilities or generators; it only balances load/generation/interchange and maintain frequency by entering schedules onto the EMS. If the intent of R1.13 is to stipulate the primary and backup control centres of a BA that balances load and generation for a BA Area of the MW size as noted in 1.13, then

#	Organization	Yes or No	Question 7 Comment
			simply say so. (5) 2.3: See our comments on 1.3. We do not see the need for this category. (6) 2.8: See our comments on 1.13. The BA does not operate transmission facilities or generators. Suggest to reword it in a similar fashion.
7.22	IRC Standards Review Committee	Yes	(i) There are "bright-line" cutoffs for the range of violations for MW of generation (1.1, 2.1) and voltage levels (1.5, 2.4). Although these cutoffs are appropriate for most of the Interconnection(s), there may be local configurations that warrant that BES Cyber System to be rated other than what is defined with the "bright-line" cutoff. CIP-010-1 should either allow for a documented alternative rating or waivers be allowed to diverge from the cutoff limits. (ii) 1.3: "Generator pre-designated as must run": In some developed markets, must run generators change from time to time and often are not determined (designated) until week/day ahead of real time. We do not believe facilities of this dynamic nature should be included. If we want to include generators having a significant impact on reliability in this category, we need only to say: "Generation Facilities that have Wide Area reliability impacts when removed from service". (iii) 1.7: Violating IROL does not result in instability, uncontrolled separation or cascading. In everyday operations, IROLs are exceeded from time to time due to changing system conditions and external impacts. For so long as such exceedances are corrected within Tv, the BES is deemed to be reliable. We suggest the first part of this category be removed. Keeping the second part "Transmission Facilities, including FACTS, that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in instability, uncontrolled separation or Cascading would suffice. (iv) 1.13: A BA does not operates transmission facilities or generators; it only balances load/generation/interchange and maintain frequency by entering schedules onto the EMS. If the intent of R1.13 is to stipulate the primary and backup control centres of a BA that balances load and generation for a BA Area of the MW size as noted in 1.13, then

#	Organization	Yes or No	Question 7 Comment
			simply say so. (v) 2.3: See our comments on 1.3. We do not see the need for this category. (vi) 2.8: See our comments on 1.13. The BA does not operate transmission facilities or generators. Suggest to reword it in a similar fashion.
7.23	FEUS	Yes	*1.1; clarify 'if the Generation Facilities capability exceeds the largest value of the Contingency Reserve or reserve sharing obligations for the Reserve Sharing Group' the Contingency Reserve is also relative to the Reserve Sharing Group. *1.10: The drafting team should consider allowing for voltage differentiations for High and Medium SPS, RAS, or automated switching stations similar to that used in 1.5 and 1.14
7.24	Hydro One	Yes	"Must run" in 1.3 and 2.3 is a phrase that we strongly disagree with, and should not be used, because it is a regulatory mechanism, and used in some areas of the country to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must run agreements. These agreements are established as a function of market payments and current grid operations, and are therefore inappropriate for establishing criteria around determining which generators impact the bulk electric system. If the Standard Drafting Team insists on using the term it must, at a minimum, define what it means by this phrase. We strongly suggest that a fourth category of NO IMPACT is included as follows: No Impact contains all other documented BES Cyber Systems that have no affect on operation and are not categorized as having either High, Medium or Low Impact rating.
7.25	Northeast Power Coordinating Council	Yes	"Must run" in 1.3 and 2.3 is a phrase that we strongly disagree with, and should not be used, because it is a regulatory mechanism, and used in some areas of the country to ensure generators receive adequate payments. Other generators - that are equally important to grid operation - may not have reliability must run agreements. These agreements are established as a function of market payments and current grid

#	Organization	Yes or No	Question 7 Comment
			operations, and are therefore inappropriate for establishing criteria around determining which generators impact the bulk electric system. If the Standard Drafting Team insists on using the term it must, at a minimum, define what it means by this phrase.
7.26	Florida Municipal Power Agency	Yes	1.1, 1.8, 1.11 and 1.13 ought to be combined into a single supply-demand mismatch metric. Also, in 1.1, 2000 MW is arbitrary and in 1.13 4000 MW is arbitrary. And in 1.11, 300 MW is arbitrary and seems to coincide with DOE reporting requirements associated with EOP-004 which has nothing to do with BES Reliability. FMPA suggests: "Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that if destroyed, degraded, misused, or otherwise rendered unavailable, can cause a supply-demand mismatch exceeding the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. Net Winter Real Power capabilities of generators are to be used in determining the supply side of determining the mismatch. The greater of actual coincident peak load, or forecasted peak load for the next year, of the Reliability Coordinator is to be used for the demand side of the equation. In the case where no Contingency Reserve or total reserve sharing obligations have been established, the supply-demand mismatch metric shall be equal to the largest loss of source plus 50% of the next largest loss of source for the Reliability Coordinator area."Such language addresses situations where a DC tie line may be the largest loss of source contingency for a region that is left as a gap in the existing definition, clarifies whether winter or summer generator capabilities are to be used, and used reliability related metrics instead of arbitrary targets. Similarly, the 1000 MW of 2.1 is arbitrary. A more appropriate metric would be the lowest expected value for a single contingency loss of source in the Reliability Coordinator area. For instance, assuming a 7% average forced outage rate for generators, using a metric of the second largest loss of source contingency in the Reliability Coordinator area for a supply-demand mismatch metric would give a greater than 99% confidence that the largest loss of source contingency at any given time is greater than that metric. Since the system is always operated to the worst case single

#	Organization	Yes or No	Question 7 Comment
			contingency at any moment, then, we would be quite confident in using the metric of the second largest loss of source contingency for Medium Impact. Hence, FMPA suggests that 2.1, 2.5 and 2.8 be combined using similar language to that which FMPA suggests for 1.1 using the second largest loss of source contingency in place of the reserve sharing obligation used in 1.1. that is:"Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that can cause a supply-demand mismatch exceeding the second largest loss of source contingency in the Reliability Coordinator Area." In 1.2, the 1000 MVARs is arbitrary. Additionally 1.2, 1.3, 1.7 and 1.10 ought to be combined using the same concept of exceeding IROLs. FMPA suggests:"Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding an IROL and/or an Adverse Reliability Impact" Similarly, the 500 MVAR in 2.2 is arbitrary. FMPA suggests combining 2.2 with 2.3 and 2.5 in a similar fashion:"Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding a SOL."Radial Facilities serving only load should not be included in 1.5 or 2.4. The term "Facilities" in these bullets is misused; a substation is NOT a Facility, but rather an interconnection point for multiple Facilities. Large auto-transformers and GSUs should not be excluded from the count. And, the distinction between the Interconnects is arbitrary and meaningless. FMPA suggests:"1.5 Transmission substations or switching stations with four or more Transmission Facilities operated at 300 kV or higher (for transformers, both primary or secondary winding > 300 kV, or a GSU of a registered generator)."By using the term Facilities, which by definition is a "... single BES Element", we also exclude radial serving only load Elements since those Elements are not Facilities. 2.4 would then be identical except using the 200 kV metric instead of 300 kV.In 2.6, the

#	Organization	Yes or No	Question 7 Comment
			distinction between the Interconnects is arbitrary and meaningless. The 300 kV metric should be used for all Interconnects. Black start and cranking paths should not be High Impact at all. High impact would be the system going black, a delay in restoring the system is a Medium Impact since the damage has already been done. Hence, 1.4 and 1.6 should be combined and made a Medium Impact. 1.14 is ambiguous. Is a tapped substation included in the count? Or a station on the end of a radial line? FMPA suggests associated the count of substations with 2.4, i.e.:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations identified in 2.4, or functionality that remotely controls a BES Cyber System with a High Impact Rating."
7.27	Southwest Power Pool Regional Entity	Yes	1.1: The criteria to include as High only the generation that exceeds the Contingency Reserve or reserve sharing obligation effectively removes nearly all generation resources from this impact category. 1.3: "Wide Area reliability impacts" as defined by the NERC Glossary of Terms (April 20, 2010) may be far too broad. If the unit is designated as RMR, it should be High impact regardless of the wide area consideration. 1.10: Please define the term "local area." 1.12 and 1.13: The Reliability Coordinator, and in the instance of a consolidated Balancing Authority, the Balancing Authority functions afforded a High impact categorization are fed real-time operational data from smaller, lower impact BES Cyber Systems owned and operated by other entities. Because of the criticality of the Reliability Coordinator and Consolidated Balancing Authority's near total reliance upon external real-time data sources, those sources need to also be afforded a High impact category. In particular, these BES Cyber Systems would include the EMS/SCADA and ICCP subsystems found in an entity's control center. 2.1: The 1000 MW criteria defining a Medium Impact generation asset will likely place

#	Organization	Yes or No	Question 7 Comment
			most generation into a Low Impact category.
7.28	Oncor Electric Delivery LLC	Yes	1.10 needs to better define “local area” (eg. 3 busses) Need criteria for “Low” such that “None” is the lowest level of protection required. Also, there is a need to have categories for systems with no IP communication or dial-up only communications.
7.29	LCEC	Yes	2.4 Replace transmission facilities with “Substations and/or switching stations and two or more non-radial transmission lines”. or”Transmission Facilities with four or more non-radial transmission lines operated at 200 kV or above in the Eastern and Western Interconnections, or 100 kV or above in the Texas and Quebec Interconnections, not included in Section 1.” 2.7 change to "non-radial" Transmission substations or switching stations or”Primary or Backup Control Centers that remotely control two or more Transmission substations or switching stations, each with four or more non-radial transmission lines, operated at 200 kV or above in the Eastern and Western Interconnections and 100kV or above in the Texas and Quebec Interconnections, or functionality that remotely controls a BES Cyber System with a Medium Impact Rating, not included in Section 1.”
7.30	Turlock Irrigation District	Yes	Attachement II criterion #1.4 states that BES Cyber Systems that can affect operations for Blackstart Resources in the Transmission Operator's restoration plan shall be categorized as High Impact. This should be changed to include only the Blackstart Resources in a region's Blackstart Capability Plan because Transmission Operator's restoration plans typically include Blackstart Resources that are not material to the restoration of the BES. Blackstart Resources that are material to the restoration of the BES are designated by each Regional Entity in accordance with NERC Standard EOP-007-0 titled "Establish, Maintain, and Document a Regional Blackstart Capability Plan". We suggest that the wording of criterion #1.4 be changed to "Generation Facilities designated as Blackstart Resources in the Regional Blackstart Capability Plan". Making this change would maintain consistency between the Standards and would also be consistent with the Purpose section of CIP-010-1 which states that the categorization of

#	Organization	Yes or No	Question 7 Comment
			BES Cyber Systems should be "commensurate with the adverse impact... on the reliability of the BES. Attachment II criterion #1.6 uses the term "primary Cranking Path". What is the meaning of the word "primary" as used in this context? We suggest that the wording be changed to "Facilities required to support Cranking Path(s) that are material to the restoration of the BES as used in a Transmission Operator's restoration plan per EOP-005".
7.31	Garland Power and Light	Yes	Attachment II 1.4 Should state that it is the Primary Black Start Unit and does not include the Next Start Unit.1.5 Multiple circuits between two substations should count as a single transmission line. General Comment Need to add “scoping filter” as described on slide 31 of the NERC Workshop (May 19-20) Presentation on CIP 10 as presented by Jackie Collett. There already has been a Regional Entity Auditor make a presentation that he intended to audit beyond the scope of what is in the current standard - he (the auditor) may apply the same approach to the new standard if the filter is not stated with the definition - not adding the clarification (scoping filter) just adds the potential for alleged violations and all the baggage that goes with that until one can hopefully get resolved - If you add the filter which states “typically excludes business, market function systems, and non real-time systems”, then it is a good scope and we would agree
7.32	Powersouth Energy Cooperative	Yes	CIP-010 Attachment II 1.1 As drafted, if reserve requirements have not been established for an entity, generation facilities are considered High Impact if singularly or in combination exceed 2,000 MW. It seems to be reasonable to apply the 2,000 MW limit to reserves as well with reserve requirements only greater than 2,000 MW being considered as High Impact. 1.4 Additional consideration should be given to categorizing blackstart units in all cases as High Impact. Some units, while identified in a TO’s restoration plan, are not part of

#	Organization	Yes or No	Question 7 Comment
			the Regional Entities Restoration Plan. Some generation that may be used in a restoration effort may be removed from the TO's restoration plan to avoid implementation of High Impact security requirements. Some "middle ground" should be found so that more units can remain available in a restoration plan without being subject to costly security requirements and subsequently an increase in exposure for a utility to be non-compliant. It is recognized that there must be a sufficient number of blackstart critical units that remain protected by High Impact status to ensure restoration following an event. 1.10 Is "local area" meant to be the Balancing area or can the entity define local area. 2.1 As drafted, if reserve requirements have not been established for an entity, generation facilities are considered Medium Impact if singularly or in combination exceed 1,000 MW. It seems to be reasonable to apply the 1,000 MW limit to reserves as well with reserve requirements only greater than 1,000 MW being considered as Medium Impact. 3. Some consideration should be given to providing exclusions to exempt assets that in reality have no material impact.
7.33	City Utilities of Springfield, Missouri	Yes	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
7.34	MidAmerican Energy Company	Yes	Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term; however, "primary Cranking Path" is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Larger entities submit multiple plans with many blackstart units and cranking paths. Protecting all blackstart units will divert valuable renounces from (better) protecting more valuable facilities. Draft definition of "primary Cranking Path": "Cranking Path and facilities included in the Transmission Operator's restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load". Subsequently, CIP-010-1 Attachment II item 1.4 should be updated to only designate

#	Organization	Yes or No	Question 7 Comment
			Generation Facilities associated with the “Primary Cranking Path”. ALSO Mr. Scott Mix indicated in the May workshop that there should not be any CIP-002 critical asset systems that map to the CIP-010 low category. Current MW ratings in Attachment II Items 1.1 and 2.1 are set too high and will cause critical generating plants to move to the low impact category. Four critical units at MEC would move to low. Simultaneous loss of the four MEC units would impact the reliability of the BES. Set the MW level in Attachment II Item 1.1 to 500MW and Item 2.1 to 300MW.
7.35	PacifiCorp	Yes	Comments: Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term; however, “primary Cranking Path” is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Larger entities submit multiple plans with many blackstart units and cranking paths. Protecting all blackstart units will divert valuable renounces from (better) protecting more valuable facilities. Draft definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load”. ALSO "Wide Area" impacts need to be clarified in Item 1.3 for "Must Run" units. ALSO Mr. Scott Mix indicated in the May workshop that there should not be any CIP-002 critical assets that map to the CIP-010 low category. Current MW ratings in Attachment II Items 1.1 and 2.1 are set too high and will cause critical generating plants to move to the low impact category. Set the MW level in Attachment II Item 1.1 to 500MW and Item 2.1 to 300MW.

#	Organization	Yes or No	Question 7 Comment
7.36	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Yes	Concerning generation facility capability, "rated net Real Power" can produce fictitious numbers that will never be attained. This should be the historical or commissioning test maximum net Real Power continuous output, whichever is greater. Wide Area is a very large area for WECC, as WECC is the RC. We are not sure if there are any generation facilities in WECC that have an impact on the whole of WECC. We are also not sure if generation being "pre-designated as reliability 'must run'" is a practice in all areas. It is possible that some units may be designated using other terminology or have detailed contracts. It may be better to remove the quotes and define Must Run Generation in the Glossary. Not all generation that is designated by the Transmission Operator's restoration plan as Blackstart is critical to the plan. It may be listed as a possible resource, but not a primary first choice. Further, much of the restoration plans are out of date and due for revision; requiring generation owners and operators to upgrade for CIP compliance only to have their plant removed in the new restoration plan in the next year or so would be wasteful. The purpose of a Blackstart resource in an old (pre-mandatory reliability standard compliance) restoration plan may be for local level of service resource for the TOP's local distribution area rather than a resource for BES reliability, i.e. the old plans to not coordinate well with each other. Last of all, should there not be a rating qualifier?
7.37	Detroit Edison	Yes	Criteria 1.3 and 2.3 should be removed for the following reasons: 1. The term "reliability must run" is not defined. 2. There is no generator that is so essential to reliability that it would need to run 100% of the time. 3. A generator could be required to run on a given day to serve load in an area that cannot be otherwise served due to a transmission constraint. This would be a temporary condition and should not warrant a high or medium classification.
7.38	Cogeneration Association of California and Energy Producers & Users	Yes	Criteria 2.4 should be clarified. The criteria states "Transmission Facilities with four or more transmission lines operated at 200kV or above..." Do two transmission lines, each with two circuits that can operate independently for a total of four circuits, count as two

#	Organization	Yes or No	Question 7 Comment
	Coalition		transmission lines or four transmission lines?
7.39	Exelon Corporation	Yes	Each of the criteria needs to either align with the other existing standard requirements, or have a technical basis or business risk mitigation basis to be defined as criteria. It would be very beneficial to the industry's understanding of each requirement if the basis for each was included in the Attachment. A specific example is the 4 or more Transmission line requirement. The previous draft had a 3 or more Transmission line requirement, so what was the basis for the 3 or more and, moreover, what is the basis for now changing it to 4 or more? The technical basis for generation limits in Attachment II is not provided. That is, the basis for the 2000 MW and 1000 MW thresholds appear arbitrary. Combined losses of greater than these values have occurred without significant impact to the BES. No "reasonable bounds" are allowed. For example, if a common vendor provides a cyber product in multiple generating stations, it appears that the assumption is that this common product, no matter how local its impact, creates a common mode failure for all plants simultaneously, resulting in the determination before the fact that this product will be rated as High Impact. No allowance is made for geographical location. For example, if a common cyber system is used in several large generating stations in different regions of the country, their simultaneous loss may result in no significant impact to the BES. However the deterministic MWe thresholds and simple "in combination" wording will result in virtually all such cyber systems rated as high, deterring use of common vendors, standardization, and economies of scale. Although moving to a more deterministic approach can be seen as increasing consistency in application of the standard, it would appear that a deterministic approach will decrease the flexibility of operation now allowed and may in fact, reduce BES reliability. As a modification to the Attachment, Exelon suggests that the existing deterministic criteria could be used, unless an entity chooses to show by actual historical data or modeling that such losses do not result in significant impact on the BES. This performance-based criteria could be expanded to define high, medium, and low impacts on the BES in terms of stability, voltage swing, etc.

#	Organization	Yes or No	Question 7 Comment
7.40	American Transmission Company	Yes	For R1.4, we propose changing text from “designated as Blackstart Resources” to “designated as the primary Blackstart Resources” (similar to primary Cranking Path in 1.6). Add “restoration plan per EOP-005” (similar to 1.6). Note that Transmission Operators can only designate Blackstart Resources that have been volunteered to them by Generation Owners. All GO may choose not to volunteer any Blackstart Resources if they don’t want their associated cyber systems to be subject to this standard. For R1.10, we propose removing SPS from the criteria. SPSs cannot be approved by the Regional Entities unless they have been designed not to be critical to the BES (e.g., not critical if they operate when they should not or do not operate when they should).
7.41	SCE&G	Yes	How does the SDT see AGC coming into play in 1.1? Would every generator operated on AGC (if the aggregated total met the contigency reserve commitment) be considered high impact, or just the centralized AGC itself?" Must Run" units needs to be clarified. Who determines if a unit is "must run"? 1.4 This language needs to be clarified to identify resources designated as "Primary" Blackstart resources. 1.5 Transmission lines should be change to Transmission Lines to utilize the NERC Definition 1.8 Is this misusing/destroying one Transmission Facility at a time? SDT should consider defining "Transmission Facility" as a whole instead of utilizing separate NERC Definitions for "Transmission" and "Facility"
7.42	Entergy	Yes	If “size” of an electric facility remains the primary key differentiator for applicability of CIP requirements, which Entergy does not support, the following should be considered: 1. High Impact Rating (H)”Each BES Cyber System that can affect operations for: 1.1. Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power

#	Organization	Yes or No	Question 7 Comment
			capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group . In the case where no Contingency Reserve or total reserve sharing obligations have been established, Generation Facilities , singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to the most current rated net Real Power capability of 2,000 MW." Attachment II of CIP-010-1 qualifier 1.1 as stated above includes those generation facilities that have the capability to exceed the Contingency Reserve as High Impact to the BES. This is not truly indicative of the impact to the reliability to the BES. Entergy has multiple generation facilities with the capability to exceed the contingency reserve. However, their Service Hours (SH) are less than 900 hours and a Service Factor (SF) is less than 1.0, averaged over the past five years, where: - Definitions from GADS Data Reporting Instructions - January 2010- Service Hours - SH is the sum of all Unit Service Hours.- Period Hours - PH is the number of hours in the period being reported that the unit was in the active state.- Service Factor - SF = SH/PH x 100% Entergy proposes that a better representation for how much a generation plant runs, and therewith potential adverse impact on BES reliability, would be better determined by a measurement of the percent of SH, e.g., running at least 80% of the year; SH greater than 7008 hours per year, or, a SF of greater than 80% per year. Therefore, suggested alternative language for 1.1 is: "Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation facilities the unit with the highest Service Factor is used to determine applicability), whose Service Factor (Service Factor = Service Hours per Year / Hours per Year X 100%) is equal or greater than 80% for a five year average." Additionally, extending this logic to the Medium Impact BES Cyber Systems, Entergy suggests replacement of language concerning Medium Impact Rating (M) 2.1 from: "Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate higher of the most current and prior to most current rated net Real

#	Organization	Yes or No	Question 7 Comment
			Power capability of 1000 MW or more, not included in Section 1." To: "Generation Facilities, singularly or in combinations (if using a shared BES Cyber System that affects multiple generation facilities the unit with the highest Service Factor is used to determine applicability) with equal to or greater than 70% for a five year average."
7.43	Edison Mission Marketing and Trading	Yes	If we are going to use the High, Medium, and Low and there is not going to be a does not apply category, then there should be an engineering analysis or study performed by the BA's, RC's or an independent firm and it should include which sites/generators are critical and which are not and why. Once completed then and only then do we begin categorizing them into whatever scale the Standard Drafting Team and the included entities agree upon. As it is stands now we not only have to include nominal size generators, but wind sites as well.
7.44	Puget Sound Energy	Yes	In 1.6, the restoration plan is linked to EOP-005, shouldn't the restoration plan mentioned in 1.4 be linked to EOP-005 as well? It appears that all BES Cyber Systems must fall into one of three categories. Are there any other criteria that would all for something not to be categorized as one of these three (i.e., such as non-dispatchable wind generation)? Also Blackstart should only classify as high those needed for primary region wide restoration since some (such as ours) are more secondary paths and there should be some minimum level of generation to be classified low. There is no need to classify as low a 20 MW hydro generator that does not impact BES reliability. We would recommend 300 MW.
7.45	Alliant Energy	Yes	In Article 1.3 we believe including "must-run" as listed is problematic. This could fluctuate in response to maintenance outages on lines, etc. The must-run units have to be tied to a long-term study that shows the need for a reliability must-run unit, not short-term analyses to reflect changing conditions.

#	Organization	Yes or No	Question 7 Comment
			Article 1.4 - By including "All Black-Start Units" the standard is utilizing a "one-size-fits-all" strategy that the industry has recognized does not work for everything, and is working to address. All Black-Start units do not carry the same importance and this should be recognized in the standard. This philosophy may be counter-productive to system reliability as one classification may reduce the number of Black Start units that would be made available to a TOP's restoration plan due to the high initial security cost and the future possible financial risk of strict compliance guidelines with penalties. There should be a recognized hierarchy for the Black-Start resources, similar to the High, Medium, and Low for BES Cyber Systems. This methodology would assure Black Start units could be categorized by attributes in general to support the BES during a blackstart event. Each Balancing Authority Area (BAA) could be required to have a minimum number of high priority Black Start units depending on the BAA size to support the area during a black out. Lower priority units would be used for stabilizing power at generating stations, local area islanded load and used as a backup plan if all other contingency plans would fail. Article 1.6 - This item should reflect the same categorizing as is recommended in the comment to Article 1.4 above. Article 2.1 - Please clarify "with aggregate higher of the most current and prior to most current rated net Real Power capability." We believe it would be clearer if stated as below: "Generation Facilities, singularly or in combination (if using a shared BES Cyber System) with a rated Real Power capability of 1000 MW or more, not included in Section 1." Article 2.3 - we believe including "must-run" as listed is problematic. This could fluctuate in response to maintenance outages on lines, etc. The must-run units have to be tied to a long-term study that shows the need for a reliability must-run unit, not short-term analyses to reflect changing conditions.
7.46	Public Service Enterprise Group companies	Yes	In general there is agreement with the R2 text. However, in Attachment II, statement 1.4 entails categorizing all Blackstart Units with a "High Impact Rating", while statement 1.6

#	Organization	Yes or No	Question 7 Comment
			requires that only the “primary cranking path” transmission facilities need to be categorized with a “High Impact Rating”. Statement 1.6 implies that some Blackstart Units, although categorized with a “High Impact Rating” would not be afforded transmission facilities with the same risk categorization. We recommend changing statement 1.6 to include only Blackstart Units that are in the primary cranking path.
7.47	ReliabilityFirst Staff	Yes	In Part 1.1, the referent for “largest value” does not seem to be appropriate. Suggest changing the wording to “average value.” In Part 1.4, a “Blackstart Resource” is only the first resource that starts in a system restoration. Suggest changing the wording to “Generation Facilities required to support the Cranking Path(s) identified in Part 1.6.” In Part 1.6, a “primary” Cranking Path is not required to be identified in an entity’s restoration plan by EOP-005. Suggest changing the wording to “Facilities required to support at least one Cranking Path.” In Part 1.10 “local area” should be defined. As we are not certain what is meant by this term, we have no suggested wording.
7.48	RRI Energy	Yes	Include or add a "No impact category" that is determined by the RC.
7.49	MRO's NERC Standards Review Subcommittee	Yes	Item 1.3 We believe this item may be problematic in nature, as the designation of reliability “must run” units is something that could fluctuate. This would create administrative difficulties for an entity and their RTO as a unit moves between Impact Ratings. We believe this item needs further clarification to indicate its true intent, such as who stipulates the “must run” designation, what constitutes “reliability must run”, etc. Item 1.4 Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator’s restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same “one size fits all” approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System.

#	Organization	Yes or No	Question 7 Comment
			Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports. We would recommend rewording item 1.4 as follows, leveraging the existing language of Item 1.8: "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.5 We need to clarify the meaning of "Transmission lines". If a 300 kV substation has a terminal connected to a 345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV "Transmission line" within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line. We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or

#	Organization	Yes or No	Question 7 Comment
			simply adding to/changing the High Impact criteria along the lines of the Medium Impact criteria (item 2.6), calling out "Transmission Facilities operated at 500 kV or higher..." Item 1.6 We would recommend rewording item 1.6 as follows for consistency in approach with the proposed Item 1.4: "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 1.1 above."We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.14 We would recommend rewording item 1.14 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System. Item 2.7 We would recommend rewording item 2.7 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, not included in Section 1."We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System. Section 2 Additions We would recommend adding the following items under section 2, Medium Impact Rating, for consistency in approach with the proposed Items 1.4 and 1.6: o "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility

#	Organization	Yes or No	Question 7 Comment
			with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." o "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.
7.50	Minnesota Power	Yes	Item 1.4: Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator's restoration plan as having a High Impact Rating with regards to the Bulk Electric System. In theory, on a smaller scale, this appears to be a "one size fits all" approach, but in reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, Minnesota Power believes that there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. To implement this approach, Minnesota Power believes it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just the fact that it has been included. For example, a 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, Minnesota Power proposes that the Standards Drafting Team allow Registered Entities to assess the relative importance of a Blackstart Resource based on the importance of the facilities it directly supports. Minnesota Power recommends rewording item 1.4 as follows utilizing the existing language of Item 1.8:

#	Organization	Yes or No	Question 7 Comment
			"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." Minnesota Power believes this approach will provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.14: Minnesota Power recommends rewording item 1.14 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."Minnesota Power believes that this approach will provide a better sense of a control center's true impact on the Bulk Electric System. Item 2.7: Minnesota Power recommends rewording item 2.7 as follows:"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, which are not included in Section 1."Minnesota Power believes that this approach will provide a better sense of a control center's true impact on the Bulk Electric System. Section 2 Additions: Minnesota Power recommends adding the following items under section 2, Medium Impact Rating, for consistency with the proposed Item 1.4:"Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."Minnesota Power believes that this approach will provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.

#	Organization	Yes or No	Question 7 Comment
7.51	The Empire District Electric Company	Yes	Item 1.4 Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator's restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same "one size fits all" approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact. A regional study performed by the regional entities would be an excellent approach to determine this. To implement this approach, we believe it is imperative to consider the Blackstart Resource's actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports. We would recommend rewording item #1.4 as follows, leveraging the existing language of Item #1.8: "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above." Since item #1.6 is also related to system restoration, we would recommend rewording it as follows for consistency in approach: "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as

#	Organization	Yes or No	Question 7 Comment
			described in Part 1.1 above." We would also recommend adding the following items under section 2, Medium Impact Rating: o "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above." o "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above." We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner. Item 1.5 We need to clarify the meaning of "Transmission lines". If a 300 kV substation has a terminal connected to a 345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV "Transmission line" within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line. We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or simply changing the High Impact criteria to mirror that of the Medium Impact (item 2.6), calling out "Transmission Facilities operated at 500 kV or higher...".
7.52	Lincoln Electric System	Yes	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS), which address the current structure of Attachment II as proposed. However, LES believes a better overall approach would be applying

#	Organization	Yes or No	Question 7 Comment
			Engineering studies to truly determine a facility's impact on the Bulk Electric System. We realize an Engineering study is not as simple as a "bright line" based metric. Unfortunately, the Bulk Electric System is not a simple system - it is actually very complex. So in order to properly assess the importance of the various facilities that make it up, LES feels a complex Engineering study is required.
7.53	Luminant	Yes	Medium Impact: an item for TO, TOP, GO, GOP Functions performed at primary or backup control centers has been left off of attachment 2. This was in the previous posting as item 2.6"Control Centers and backup Control Centers controlling transmission ...
7.54	Nuclear Energy Institute	Yes	Need to clarify the expectations for a multi unit generation site. For example: Under what conditions would a site containing two separate 900 MW generators be considered "Medium Impact Rating" because the total site would now be greater than 1000 MW? Similarly, when would a site that had three separate 900 MW generators be considered "High Impact Rating" because the total site would now be greater than 2000 MW?
7.55	NextEra Energy Corporate Compliance	Yes	NextEra finds that a catch-all for Low impact is a fatal flaw. There should be some threshold that is justified for low. For example, a proper minimum criteria for LOW impact BES Cyber Systems could be:Cyber Systems that control BES level facilities that meet one of the following: 1) three or more transmission circuits operated at 100 kV or above not covered in Section 1 or 2, 2) two or more transmission circuits and two or more autotransformer with a secondary voltage 100kV or above,3) two or more transmission circuits and generation capacity at the site of greater than 1000MW Alternatively, a NO IMPACT category may be added which eliminates subjectivity in which BES Cyber components need to be reviewed. Single point buses representing looped load serving type stations cannot produce results worse than single contingency which must be operated to at all times. An additional item that should be specifically covered is the use of remote access for transmission and / or generation control locations and their applicability to the High, Medium, Low and/or No impact criteria.

#	Organization	Yes or No	Question 7 Comment
			The term "affect operations" can be subjective and can be open to interpretation. NextEra suggests changing the15 minute requirement to “in real time (instantaneous). For example, closed loop control, which does not allow time for human intervention.” NextEra also recommends adding the word “both” prior to monitor and control. NextEra would also like to know what does 1.1.1 of section D mean? This is unclear. A suggestion would be eliminating or providing a specific definition.
7.56	Pacific Gas & Electric Company	Yes	Not all blackstart resources should necessarily be considered high impact. Suggest revising 1.4 as follows: Generation Facilities designated as Blackstart Resources and explicitly listed as essential to the restoration of the BES in the Transmission Operator’s restoration plan.
7.57	Northeast Utilities	Yes	NU is concerned with some of the impact criteria in Attachment II related to generation facilities. To base impact on “bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc., could lead to mis-categorization and ultimately unprotected cyber systems. These thresholds do not take into consideration regional differences in configuration and load flows. Therefore, it is our suggestion that categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause levels of impact to the BES.
7.58	Matrikon Inc.	Yes	Please describe how the 15-minute time horizon would fit into Attachment 2. Is the intent for the 15-minute horizon to provide a level of realism to determination of impact? To bring in more BES Cyber systems that could have indirect impact, or an escape clause if effects don’t occur within 15 minutes?
7.59	USACE HQ	Yes	Please read answer to question 4.

#	Organization	Yes or No	Question 7 Comment
7.60	BGE	Yes	Provide additional clarification of “automatic aggregate”. For instance, does automatic mean an application that is kicked off without human intervention or does automatic mean after an operator hits a button? Suggest adding the word “instantaneous” before load shedding to clarify. Additional clarification on 1.14 (What is meant by “functions”)
7.61	Southwestern Power Administration	Yes	Rather than numerous bright line requirements that may or may not actually have a significant effect on the BES, depending on the surrounding topology, operating procedures, or configuration of a particular Responsible Entity, a better approach may be to include performance/results-based criteria in Attachment II. However, if the current approach is forwarded, I would suggest the following improvements: 1.4. Generation Facilities designated as Primary Blackstart Resources in the entity’s restoration plan. 1.7 Transmission Facilities, including Flexible AC Transmission Systems (FACTS), that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more Interconnection Reliability Operating Limits (IROLs). 1.10 Special Protection Systems (SPS), Remedial Action Schemes (RAS) or automated switching systems that operate BES Elements that if destroyed, degraded, or misused, would violate one or more Interconnection Reliability Operating Limits (IROLs). 1.11. Delete. Is this not a Control Center issue? 1.12. Control Centers that perform the Reliability Coordinator functions. 1.13. Control Centers that perform the Balancing Authority functions for 4,000 MW or more in Eastern and Western Interconnections and 2,000 MW or more in the Texas and Quebec Interconnections. 1.14. Control Centers that perform the Transmission Operator functions for a Facility

#	Organization	Yes or No	Question 7 Comment
			with a High Impact Rating. 2.4. Transmission Facilities that, if destroyed, degraded, misused or otherwise rendered unavailable, would violate one or more System Operating Limits (SOLs) 2.7. Control Centers that perform the Transmission Operator for a Facility with a Medium Impact Rating, not included in Section 1. 2.8. Control Centers that perform the Balancing Authority functions for 2,000 MW or more in the Eastern and Western Interconnections and 1,000 MW or more in the Texas and Quebec Interconnections, not included in Section 1.
7.62	Southern California Edison Company	Yes	SCE believes Attachment II should be modified to account for only the capacity that can be controlled by qualifying systems. As currently written, Attachment II defines the amount of generation under control as the rated capacity of the resource. This is not accurate for some systems which can only control the resource between certain points (e.g. minimum operational output [Pmin] and maximum operational output [Pmax]). This could drastically overstate the impact of the cyber system on the BES. For example, suppose that a cyber system controlled a generating resource with maximum capacity of 2,000 MW. According to attachment II, this would then categorize as "high impact rating". However, suppose further that the system can only control the unit between its Pmin and Pmax which are 1,500 and 2,000 respectively. This would place the system in a "low impact rating" according to the attachment. For that reason, SCE believes that Attachment II should be modified to account for only the capacity that can be controlled by the system.
7.63	San Diego Gas and Electric Co.	Yes	SDG&E recommends aiming for a limitation of scope related to those assets that are truly high and medium impact categorizations. Some of the high and medium items could have "BES outage" or reliability implications but may not necessarily result in instability of the BES. We recommend having consistency in the application of the assets included in the impact categories to the BES as a whole.

#	Organization	Yes or No	Question 7 Comment
7.64	Constellation Energy Control and Dispatch, LLC	Yes	See answer to Question 4.
7.65	Constellation Energy Commodities Group Inc.	Yes	See answer to Question 4. Please clarify the intended treatment of a Generation Management System ("GMS"). Attachment II implies that capacity monitored by a GMS system would be aggregated to determine its impact categorization. However, to be consistent with the intention to protect connections that truly impact the BES net real power capability should only be aggregated within a balancing authority.
7.66	MWDSC	Yes	See comments for question 4 above.
7.67	Wolverine Power	Yes	See comments listed for 1.a
7.68	Dynegy Inc.	Yes	Show examples of how the identification and categorization and tie-in to Attachment II would work.Also, for 1.1, either increase the net MW rating or add an annual capacity factor to a generating unit to account for old units at a site that no longer run because no longer economical. These types of facilities should not have to meet High category requirements if they no longer run. Also, for 1.3 add more detail. Explain pre-designated. Assigned by who? Explain Wide Area reliability impacts.
7.69	WECC	Yes	Similar to our previous comment, if Attachment 1 is expanded to include in scope reliability coordination functions critical to reliable operation of the BES outside of 15 minutes the impact levels need to be updated. While many functions of a Reliability Coordinator are critical and should be an high impact, not all functions of reliability coordination should be made high impact. For instance, Coordinated Outage systems while important to the reliability of the BES and should be in scope, should best be classified as a low-impact BES Cyber System. The considerations for identification and categorization has been elevated to a high level such that BES Cyber Systems and not individual devices are identified based on their specific functionality. It is suggested that if BES Cyber Systems are to be indentified and

#	Organization	Yes or No	Question 7 Comment
			categorized there be some inclusion and development of a process to granulate these systems down to their individual component level. Further, the quantitative qualification bar has been set to level that precludes most BES Cyber Systems from reaching identification as a high or even medium level of impact. Taking into account. If a BES Cyber System can impact reliability a baseline set of security controls should be established that creates tracking for all assets, accountability for access to these assets, and physical and electronic protection for these assets. Specific Line Item Comments(1.1) The standard, as drafted, seemingly excludes all generation but large dams, large mine-based coal plant and nuclear plants?(1.1) The developed sentence structure lends itself to multiple interpretations and will prove to be difficult to audit consistently. (1.1) Is the term aggregated defined as geographically co-located, common substation, common communication paths, etc?(1.6) What about redundant paths? There is no requirement to identify and document multiple paths. (1.6) A reference to EOP-008 would also be appropriate.
7.70	Con Edison of New York	Yes	Specific comments on the Categorization: The impact categories should be linked to the reliability Standard functions in Attachment I. Therefore, the High, Medium and Low ratings should reference specific Standards whenever possible. o 1.1: This requirement should be broken down into two requirements. One should refer to BAL-002 and reserves needed to be compliant. The second should be any generation facility with a common BES Cyber System greater than 2,000 MW. o 1.2: This should be linked to the function of “controlling voltages”. Two other concerns; first - shunt reactors and capacitors are not included and second - there needs to be a technical basis for a Reactive Power capability limit. o 1.3: Suggest moving to “Low” category since reliability must run equipment is frequently a local congestion or voltage control situation. This would not qualify for a “High” impact rating.

#	Organization	Yes or No	Question 7 Comment
			o 1.4: Black start resources should only be designated as a High Impact Rating if they are the only resource in the TOP's restoration plan. If the TOP has multiple restoration resources and procedures, the resources should be a Medium Impact Rating. Reference this to EOP standards. o 1.5: OK o 1.6: This item should be included in item 1.4 o 1.7: FACTS devices are used to control voltage and power flow. o 1.8: This should be included in requirement 1.1 o 1.9: OK o 1.10: Refer to PRC standards o 1.11: A basis for the 300 MW or greater UFLS system should be provided. o 1.12, 1.13, and 1.14 address Control Centers and should be aggregated into one requirement based on RC functions, BA functions, TOP functions and TO functions. In addition, there may be a conflict between a Control Centers with a "Low Impact Rating" and a single substation with a "High Impact Rating". The DT should consider addressing this conflict where the "BES Cyber Security Components" on one side of a device (e.g. breakers) is a "high impact" while the command signal will be a "low impact" device. General comment on criteria for categorization: Overall, the high, medium, and low levels do not properly meet the needs of the BES. The DT should be looking at what the system does and determining its ability to impact the BES rating rather then the impacted equipment. For example, SCADA systems should be High whether they are on the 138 kV or 345 kV. Wide scale damage can be done with access to the SCADA system, however only local issues can occur with access into a single non-networked microprocessor relay. Alarm panels and other microprocessor that do not have direct impact should also be at lower level. Items that set levels should be a medium level. Basis for criteria for categorization is needed:

#	Organization	Yes or No	Question 7 Comment
			Attachment II to CIP-010 contains a number of what appear to be administratively determined "bright lines." Please provide both the detailed rational supporting each "bright line" and a specific quantification of the reliability benefits resulting from its implementation. In responding to this question, please focus more on the technical, reliability-related rational and improvements for each "bright line" selected, rather than on the source of any particular number. Reference any white papers, studies, expert opinion, or other documentation relied upon and supporting the "bright lines" selected. For example, in Attachment II category High Impact for item 1.11, please explain why 300 MW was selected. We are not so much interested in any reference to a 300 MW EOP-004 DOE reporting requirement, as we are in the specific criticality of the 300 MW level to BES reliability, e.g., 300 MW represents a large (>10%) percent of area load, or in the case of inadvertent actuation would cause an uncontrolled system instability(ies) and cascading, or in the event of a failure-to-actuate would cause the Interconnection UFLS program not to return frequency to nominal within the program required time period. What if for a given entity 300 MWs is not a significant percentage of local load, or inadvertent actuation would not cause uncontrolled instability and cascading, or failure-to-actuate would not prevent the return of frequency to normal within the required time period? Why rate such aggregate automatic load shedding "High" rather than "Medium" or "Low?" Are there any Interconnection-wide studies which would support this 300MW "bright line" value? Please provide any reference(s).
7.71	Allegheny Energy Supply	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact.

#	Organization	Yes or No	Question 7 Comment
7.72	Allegheny Power	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, “primary Cranking Path” is not defined. Item 1.3 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from (better) protecting more valuable facilities. Moreover, it is not appropriate to create a perverse incentive for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. Draft definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for restoring the BES system to a stable condition with sufficient generation capacity synchronized to complete the full restoration of native load”. Regarding 1.7, we recommend striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does not appear in the NERC Glossary of terms The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. Under Frequency Load Shed systems under a common control system.

#	Organization	Yes or No	Question 7 Comment
7.73	EEI	Yes	Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. Clarification is needed for the term “primary Cranking Path” (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term, however, “primary Cranking Path” is not defined. Item 1.4 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. As a result, the drafting team should consider whether to combine Items 1.4 and 1.6. Moreover, most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from providing additional protections for more valuable facilities. Moreover, this may create incentives for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. It is not appropriate to expand the definition of blackstart to include full restoration of native load, that would essentially include all or most of the BES. The objective here is to prioritize, and augment security for the elements needed to begin system restoration. EEI suggests the following definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for initial system restoration”. In addition, the drafting team should modify the wording to only include units designated on a seasonal or annual basis. Regarding 1.7, EEI recommends striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does

#	Organization	Yes or No	Question 7 Comment
			not appear in the NERC Glossary of terms Suggest Adding: 1.15 Control Centers including Generation Control Centers. Also, we suggest that the drafting team place the highest impact facilities earlier (e.g. 1.1) on the list. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. EEI suggests that 1.11 in Attachment II be revised as follows:"BES Elements that perform automatic aggregate load shedding of 300 MW or more under a common control system."]
7.74	APPA Task Force	Yes	The APPA Task Force commends the drafting team on their work on CIP-010-1. We appreciate the team's consideration of our Task Force comments from the previous informal comment period. We feel it is especially important for entities to have the option of categorizing the impact level based on the Contingency Reserve or total of reserve sharing obligations as stated in 1.1. However, we are concerned with the "bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc. These thresholds do not have a basis from industry experience and could be challenged by entities or regulators. We are concerned that having chosen these numbers without empirical data supporting them, the numbers can easily be changed without the supporting empirical data. It is our recommendation that these numbers be evaluated more closely. At a minimum, the thresholds should be quantified to show what percentage of generation and transmission facilities would be designated under each Impact Rating. Florida Municipal Power Association (FMPA) provided some suggested alternative calculation methods for the Impact Categorization of Attachment II. We provide them here for the drafting team's discussion in evaluating the bright line thresholds. FMPA Comments:

#	Organization	Yes or No	Question 7 Comment
			Categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause the following levels of impact to the BES: o High (has the potential to cause an Adverse Reliability Impact) o Medium (has the potential to require planned/controlled loss of load) o Low impact (has no potential to cause loss of load) Make changes to existing criteria: 1.1, 1.8, 1.11 and 1.13 ought to be combined into a single supply-demand mismatch metric. Also, in 1.1, 2000 MW is arbitrary and in 1.13 4000 MW is arbitrary. And in 1.11, 300 MW is arbitrary and seems to coincide with DOE reporting requirements associated with EOP-004 which has nothing to do with BES Reliability. FMPA suggests: “Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that if destroyed, degraded, misused, or otherwise rendered unavailable, can cause a supply-demand mismatch exceeding the largest value, for the 12 months preceding the categorization, of the Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group. Such language addresses situations where a DC tie line may be the largest loss of source contingency for a region that is left as a gap in the existing definition, clarifies whether winter or summer generator capabilities are to be used, and used reliability related metrics instead of arbitrary targets. Similarly, the 1000 MW of 2.1 is arbitrary. A more appropriate metric would be the lowest expected value for a single contingency loss of source in the Reliability Coordinator area. For instance, assuming a 7% average forced outage rate for generators, using a metric of the second largest loss of source contingency in the Reliability Coordinator area for a supply-demand mismatch metric would give a greater than 99% confidence that the largest loss of source contingency at any given time is

#	Organization	Yes or No	Question 7 Comment
			greater than that metric. Since the system is always operated to the worst case single contingency at any moment, then, we would be quite confident in using the metric of the second largest loss of source contingency for Medium Impact. Hence, FMPA suggests that 2.1, 2.5 and 2.8 be combined using similar language to that which FMPA suggests for 1.1 using the second largest loss of source contingency in place of the reserve sharing obligation used in 1.1. that is: ”Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple Facilities) or Control Centers that can cause a supply-demand mismatch exceeding the second largest loss of source contingency in the Reliability Coordinator Area.” In 1.2, the 1000 MVARs is arbitrary. Additionally 1.2, 1.3, 1.7 and 1.10 ought to be combined using the same concept of exceeding IROLs. FMPA suggests: ”Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding an IROL and/or an Adverse Reliability Impact.” Similarly, the 500 MVAR in 2.2 is arbitrary. FMPA suggests combining 2.2 with 2.3 and 2.5 in a similar fashion: ”Transmission Facilities, active compensation devices (such as synchronous condensers and SVCs), reliability must-run generation, or Special Protection Systems, that, if destroyed, degraded, misused, or otherwise rendered unavailable, results in exceeding a SOL.” Radial Facilities serving only load should not be included in 1.5 or 2.4. The term “Facilities” in these bullets is misused; a substation is NOT a Facility, but rather an interconnection point for multiple Facilities. Large auto-transformers and GSUs should not be excluded from the count. And, the distinction between the Interconnects is arbitrary and meaningless. We suggest:

#	Organization	Yes or No	Question 7 Comment
			”1.5 Transmission substations or switching stations with four or more Transmission Facilities operated at 300 kV or higher (for transformers, both primary or secondary winding > 300 kV, or a GSU of a registered generator).” By using the term Facilities, which by definition is a “... single BES Element”, we also exclude radial serving only load since that those Elements are not Facilities. 2.4 would then be identical except using the 200 kV metric instead of 300 kV. In 2.6, the distinction between the Interconnects is arbitrary and meaningless. The 300 kV metric should be used for all Interconnects. 1.14 is ambiguous. Is a tapped substation included in the count? Or a station on the end of a radial line? FMPA suggests associated the count of substations with 1.5, i.e.:”Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more Transmission substations or switching stations identified in 1.5, or functionality that remotely controls a BES Cyber System with a High Impact Rating.” End of FMPA comments. The APPA Task Force also supports the proposal by the MRO-NERC Standards Review Subcommittee (MRO-NSRS) in their comments on Item 1.4 and 1.6 to assign the impact rating of blackstart units and cranking path relative to assigned impact rating of the generating facilities it directly supports. We feel that inclusion of all blackstart resources in the High Impact Rating will waste limited resources protecting facilities which are not in support of High Impact generation. MRO-NSRS proposal: High Impact:1.4 “Generation Facilities designated as Blackstart Resources in the Transmission Operator’s restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above.” 1.6 “Facilities required by the Transmission Operator’s restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated

#	Organization	Yes or No	Question 7 Comment
			capabilities as described in Part 1.1 above."Medium Impact:2.X "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1." 2.X "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."
7.75	US Bureau of Reclamation	Yes	The criteria defined in this and several previous requirements are based around BES Cyber Systems, which under the definition of BES (per the WECC Glossary) does not include all power system assets. Therefore, there appears to be a category of Cyber Assets that do not presently require any protection measures (i.e., they might control a powerplant feeding a radial load or be associated with a system of less that 100kV. The classification "Low" will potentially include those systems which do not have an impact. It is counterintuitive to classify a system as low when it has No Impact. The Team should develop a description of "Low" similar to that which was provided for "High" and "Medium". Then the Drafting Team could issue a statement that systems not classified as "High", "Medium" , or "Low" would be classified as "No Impact".
7.76	Dominion Resources Services, Inc.	Yes	The criteria for categorization of Low Impact systems is too broad and uses the terminology "can affect" which the SDT has appropriately recognized is ambiguous. The following alternate wording is proposed:"All other BES Cyber Systems not categorized as having a High or Medium Impact rating that are required for the reliable operation of the BES."
7.77	Southern Company	Yes	The definition of "pre-designated as Reliability must run" in Attachment II, 1.3 is unclear and cannot be implemented with existing practices in some utilities. For utilities who designate units as must run on a day-ahead basis in some cases, a valuable practice, every unit in the fleet would have to be classified as high impact. The wording should be changed to only include units designated on a seasonal or annual basis. In addition, a

#	Organization	Yes or No	Question 7 Comment
			definition of “must run” should be provided or referenced from elsewhere in NERC documentation. The wording in 1.3 also creates a new requirement that all “must run” units be classified as to whether they have Wide Area impact, which is not currently required. Are there actually any “must run” units (or any units, for that matter) that have Wide Area impact? Because Blackstart Resources are included in Cranking Paths, 1.4 is redundant in light of 1.6 and should be removed. Alternatively, 1.4 should be limited to primary Blackstart Resources to match 1.6. In 1.4, consideration should be given to reducing the impact level for situations where multiple Blackstart Resources are available. Universally search for “effect” and replace with “adverse effect”. In 1.6, replace “support” with “is part of”.In 1.7, delete the phrase "including Flexible AC Transmission Systems (FACTS). This is redundant as it is referenced again in the following sentence.
7.78	Constellation Power Source Generation	Yes	The final sentence in 1.1 needs to be rewritten, as it’s extremely confusing. A suggestion would be to simply add the 2,000 MW bright-line at the end of the first sentence. It would read “Generation Facilities, singularly or in combination (if a singular BES Cyber System that affects multiple generation Facilities), whose aggregate rated net Real Power capability exceeds the largest value, for the 12 months preceding the categorization, of the Contingency Reserve, total of reserve sharing obligations for the Reserve Sharing Group, or 2000 MW (if no Contingency Reserve or total of reserve sharing obligations for the Reserve Sharing Group is established).” Is it the intent of the SDT for the MOD10 data to be the data used in this criteria? If so, that data changes seasonally, so a seasonal review would be needed, especially for units who are on the thresholds of the high/medium/low criteria. A suggestion would be to use nameplate data as that is a fixed rating that will not change. 1.4 and 1.6 should be

#	Organization	Yes or No	Question 7 Comment
			combined together, as they are referring to similar items. The combined High Impact Rating should read "Generation, Transmission, and other Facilities required to support a primary Cranking Path used in a Transmission Operator's restoration plan per EOP-005." However, 1.4 and 1.6, either combined or separate, still penalize generation entities that own numerous black start facilities within a single Balancing Authority's footprint. Generation entities in the aforementioned situation have already invested a lot to ensure the reliability of the BES, but under CIP-010 they will be forced to invest even more. A suggestion would be for the TOP to designate a percentage of the black starts as High, and the rest as medium or low depending on their MW size. Another suggestion would be for the TOP to specifically designate certain black start units as high, and the rest are classified based on their MVA size, with the caveat that the TOP should not designate all black start units as high to avoid liability.
7.79	Dairyland Power Cooperative	Yes	The impact ranking for blackstart should be equivalent to the highest impact of all transmission and control center systems. If an entity has only low or medium impact systems other than blackstart, a high impact for blackstart is not appropriate. 1.2 and 2.2 specify 1000 MVAR and 500 MVAR, respectively for categorizing reactive power facilities. Since reactive power problems are localized in general, these numbers seem to be high. It is difficult to set global criteria on reactive power as it is network dependent. I would advise about 50% of the proposed level to be more conservative.
7.80	Duke Energy	Yes	The quantities identified on Attachment II appear arbitrary, and need an engineering basis. We suggest an approach based upon Violation Risk Factor language, such that for the High Impact Rating, the qualifier should be whether or not the BES Cyber System could directly cause or contribute to Bulk Power System instability, separation, or a cascading sequence of failures, or could place the Bulk Power System at an unacceptable risk of instability, separation, or cascading failures. For the Medium Impact Rating, the qualifier should be whether or not the BES Cyber System could directly affect the electrical state or the capability of the Bulk Power System, or the ability to effectively monitor and control the Bulk Power System, but is unlikely to lead to Bulk Power System

#	Organization	Yes or No	Question 7 Comment
			instability, separation, or cascading failures. Need to clarify the expectations for a multi unit generation site. For example: Under what conditions would a site containing two separate 900 MW generators be considered "Medium Impact Rating" because the total site would now be greater than 1000 MW? Similarly, when would a site that had three separate 900 MW generators be considered "High Impact Rating" because the total site would now be greater than 2000 MW? o CIP10-1.4: We have many small sites (hydro's) listed in our Blackstart plan because they are available. They are not essential to our plan, but because they are available, we list them. Under this guidance, we would be required to include them as "High Impact", when in reality they are 'Low'. The wording should be revised to reflect that only those sites "REQUIRED" for Blackstart be secured under 1.4 o CIP10-1.6: We need a defined and clear understanding of what is intended in the use of the term "Cranking Path" as it relates to CIP and EOP-005. What is being sought under this requirement? The term is loosely defined in the glossary, and how it is interpreted by the industry may vary greatly from how it is intended by regulators. o Under our current understanding of the term, we would see minimal increase in sites added to our "High" list. However if we impose a severe interpretation, we could see an exponential increase to our 'High' list. o CIP10-1.7 & 2.5: The word 'Misuse' should be removed or very strictly defined. It is too vague to have meaning. o CIP10-1.11: Need a clear and functional definition of 'Element' for the industry to understand the intent of the requirement. Current glossary definition is poor at best. Also, revise 2.6. as follows: Transmission Facilities operated at 300 kV or higher, which have 2 or more 300kV or above lines, in the Eastern and Western Interconnections or operated at 200 kV or higher in Texas and Quebec Interconnections not included in Section 1.
7.81	Bonneville Power Administration	Yes	The sixth line in 1.1 begins with the words "Generation Facilities." Generation Facilities is not a defined term in the April 20, 2010, Glossary of Terms Used in NERC Reliability

#	Organization	Yes or No	Question 7 Comment
			Standards. Since this phrase is not used at the beginning of a sentence, it should be "generation Facilities." There is the same problem at the beginning of the second line in 1.2. That should also be changed to be "generation Facilities."The first line in 1.7 contains the phrase "Flexible AC Transmission Systems (FACTS)." That phrase is not defined in the April 20, 2010, Glossary of Terms Used in NERC Reliability Standards. Aren't all capitalized terms used in Standards supposed to be defined? Or does FACTS have a generally accepted definition in the industry? CIP-010-1 - Attachment II Impact Categorization of BES Cyber Systems High Impact Rating (H)Each BES Cyber System that can affect operations for:1.1. Generation Facilities, etc."can affect operations" does not relate to impact. We suggest it be reworded: "If the BES systems can change operation by the following amounts they will be in the HIGH CATEGORY: - Generation - 4,000 MW- trip or reduce output of "MUST RUN" generators to below their MUST RUN amount. - Transmission - de-energize at least 4 lines above 300 kV - MVAR support - change MVAR by 1,000 MVAR
7.82	US Army Corps of Engineers, Omaha Distirc	Yes	The word "affect" in the first sentence is somewhat ambiguious and does not fit the intent of all of the subsequent paragraphs(1.4 & 1.6) Paragraph 1.3 define wide area impacts. Paragraph 1.4 should be limited to BES Cyber Systems that are required to energize a Blackstart Resource listed in the TO's system restoration plan per the GO's written restoration plan. As written it appears to apply to any BES Cyber System that merely affects the Blackstart asset and that all BES at such a facility would be High Impact which could have a chilling effect on an entities willingness to provide Blackstart resources. Paragraph 1.6 should be limited to BES Cyber Systems required to operate or support equipment in the primary cranking path. Again this would appear to apply to all BES Cyber Systems at such a facility merely because the facility was part of the cranking

#	Organization	Yes or No	Question 7 Comment
			path regardless of their impact on system restoration. Paragraph 1.10 define impact beyond the local area.
7.83	Midwest ISO	Yes	There is no documentation for the justification of the selection of the various thresholds. Justification of these thresholds should be documented and defended.
7.84	SRW Cogeneration Limited Partnership	Yes	There needs to be a category for "no impact". We are a small Cogen plant that does not even sell firm power to the grid. In essence, we are a steam plant that happens to generate electricity. We have no "Critical Assets" as defined by CIP-002. There needs to be an equivalent level for that in CIP-010. If there needs to be a system study performed by the RC to support a "no impact" rating, that's fine. And if a facility is found to be "no impact", then that facility should be exempt from the majority of further CIP requirements, just like today where CIP-004 thru CIP-009 do not apply to facilities with no Critical Assets/Cyber Assets and only R2 of CIP-003 applies.
7.85	Covanta Energy	Yes	There still needs to be some allowance to fewer mandatory requirements associated with smaller generators.... those in the 20-50 MW range (which are unmonitored) who typically have to notify their TOP/BA that they are on the system or off the system (or reduced load if applicable).
7.86	Pepco Holdings, Inc. - Affiliates	Yes	We agree with EEI's comments.
7.87	We Energies	Yes	We Energies agrees with EEI Suggested revision for 1.2: Synchronous condensers, static VAR compensators, capacitor banks and other Facilities not associated with Generation Facilities, singularly or in combination (if using a shared BES Cyber System), with aggregate rated net Reactive Power capability of 1,000 MVAR or more. We Energies agrees with EEI comments Clarification is needed for the term "primary Cranking Path" (CIP-010-1 Attachment II item 1.6). Cranking Path is a NERC defined term,

#	Organization	Yes or No	Question 7 Comment
			however, “primary Cranking Path” is not defined. Item 1.3 includes all generating facilities designated as Blackstart Resources in the Transmission Operator's restoration plan. Most larger entities submit multiple plans with multiple blackstart units and cranking paths. Protecting all blackstart units may divert finite resources from (better) protecting more valuable facilities. Moreover, it is not appropriate to create a perverse incentive for system owners and operators to reduce the current flexibility and diversity of multiple blackstart units and cranking paths by requiring a level of protection that is not proportional to the level of impact to restoration of the BES. It is not appropriate to expand the definition of blackstart to include full restoration of native load, that would essentially include all or most of the BES. The objective here is to prioritize, and augment security for the elements needed to begin system restoration. Proposed definition of “primary Cranking Path”: "Cranking Path and facilities included in the Transmission Operator’s restoration plan as the preferred path and facilities for initial system restoration”. Regarding 1.7, we recommend striking “Flexible AC Transmission Systems (FACTS)” because it would be included within Transmission Facilities. Although capitalized, it does not appear in the NERC Glossary of terms. We Energies agrees with EEI. Suggest Adding:1.15 Control Centers including Generation Control Centers .Also, we suggest that the drafting team place the highest impact facilities earlier (e.g. 1.1) on the list. The Standard needs a definition of Blackstart Resources that addresses, or modify the language in 1.4 to clarify, that only Blackstart Resources identified as essential to initial restoration of the BES in the TOP restoration plan are intended as High Impact. Under Frequency Load Shed systems under a common control system.
7.88	Ameren	Yes	We generally agree with the criteria used to identify “High” impact facilities, but believe that the item 1.5 criterion should be expanded to include EHV transformers, and not

#	Organization	Yes or No	Question 7 Comment
			limited to 4 EHV lines. However, there are too many EHV facilities in item 2.6 that would be classified as “Medium” impact, but should be classified as “Low” impact. It is suggested that EHV facilities with three or less EHV lines and transformers should be considered as “Low” impact, as they likely have little impact on the BES. The use of TPL performance standards would confirm that many of these facilities have a “Low” impact. For 1.1 the 4th sentence should be reworded to say "total obligations for the entire Reserve Sharing Group." 1.3 needs clarification of what a "reliability must run" unit is. Also, clarify 1.4 if it refers to the actual black start unit, or the entire plant in which the black start unit resides. Last, clarify 1.6 on what magnitude of support is required by the facility. Currently this could apply to any Transmission or Generation Sub-system in the path. Performance criteria, such as the loss of 300 MW of system load to qualify for “High” impact or 100 MW of system load to qualify for “Medium” impact, should also be applied to the EHV facilities identified in items 1.7 and 2.6.
7.89	GTC & GSOC	Yes	We recommend that Attachment II be organized to more clearly indicate which items apply to which type of assets. In the case of Control Centers, it appears the primary applicable item in the High Impact category are 1.12, 1.13 and 1.14, but several other items could be misconstrued to apply as well, which could lead to those control centers being inadvertently given a High designation.
7.90	CenterPoint Energy	Yes	While it appears the SDT put a lot of effort in the development of Attachment II, the criteria to be used is arbitrary, is too prescriptive, does not allow for studies or analysis to determine whether or not the loss, compromise, or mis-use of an identified facility would have an impact on the reliable operation of the BES and, in some cases, appears inconsistent. For example; 1.5 Transmission Facilities with four or more Transmission lines operated at 300kV of higher in the Eastern or Western Interconnections or operated at 200kV or higher in the Texas or Quebec Interconnections would require any and all facilities meeting this criteria to be categorized as High Impact without any basis for this rating. Determining a facility’s impact to an electric transmission system involves

#	Organization	Yes or No	Question 7 Comment
			more analysis than counting the number of transmission lines operated at or above a threshold voltage level; 1.14 Transmission Operator functions is based on the number of substations a control center may be able to remotely control. The previous criterion, 1.13 Balancing Authority functions, is based on the mega-watt amount the Control Center operates. Neither offers a basis for either the number of substations or the mega-watt amount under the operation of the Control Center. While CenterPoint Energy would find Attachment II useful as a guide or systems to be considered it is apparent the SDT meant this to be a requirement and therefore CenterPoint Energy does not agree with Attachment II and suggests it be deleted.
7.91	Verizon Business	Yes	1) Attachment II, Item 1.1 regarding Generation Facilities – Suggest removing any reference to "Contingency Reserve" or "Reserve Sharing Group." Specifically, any Generation Facility, singularly or in combination with aggregate higher than 2,000 MW should be included as a High Impact Rating. Reference to the "Contingency Reserve" (etc.) comments can result in incorrect or inconsistent declaration of a generation asset being a High or Medium impact. 2. What is the status of OSI Layer 3 definition raised in the FAQs of March 2006? For the definition above and for CIP-002 earlier versions, OSI Layer 2 was not included; however, the inference above is that it now is included. This and any other questions from FAQ for CIP-002 should be addressed in the standard.

8. Do you have any other comments to improve this version of draft standard CIP-010-1? If so, please explain and provide specific suggestions for improvement.

Summary Consideration:

Many entities commented on the need to have the approach provided in the posted CIP-010 and CIP-011: it was pointed out that a substantial amount of work has been done in compliance with a Risk Based Methodology. Many entities commented on the the use of the systems approach, remarking that the flexibility allowed may not be appropriate. Other entities commented that the work done in the current CIP-002 through CIP-009 with Critical Assets should be preserved.

The SDT has reconsidered its approach to the structure of the standards and believes that Version 5 will provide an incremental approach while addressing the FERC directives.

#	Organization	Yes or No	Question 8 Comment
8.1	Constellation Power Source Generation		A guidance document is needed to add clarity, as some terms are still vague.
8.2	Allegheny Energy Supply		A lot of work went into the prepration of the existing CIP-002 standard. This new CIP-010 standard completely throws away that body of work in favor of this new approach. While there are many good things about the new approach, please consider the amount of work that entities have given to refine the CIP-002 drafts and to create and implement the current identification methodoligies and compliance plans. We suggest that you consider incorporating the new ideas as incremental changes to the existing standards. Suggest that the standard require controls that are commensurate with the amount of risk of compromise that a device presents. Not all BES Cyber System components present the same risk, or if compromised, have the same potential impact on the BES. For example: - Serially attached electronic components do not face or create the same risk as those that use routable protocols. - Devices that communicate to each other within a self-contained, isolated network

#	Organization	Yes or No	Question 8 Comment
			segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. - Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.3	Entergy		A) Giving each individual Responsible Entity the 'freedom' to define "a system" any which way each prefers will almost certainly create similar problems as those experienced with CIP-002-1/2/3 that allowed each Entity to chose a 'risk based assessment methodology' of its own preference to identify Critical Assets. In the abstract the notion of self-conceptualization of "a system" may be appealing, but in terms of the confusion factor relative to NERC's goals for consistent interpretation, application, and subsequent audit-ability across the industry this portends trouble. Entergy suggests that "BES Cyber Systems" should be defined as collections/groups of hardware and software employed cooperatively to execute a Reliability Function in Attachment I. It is not necessary to explicitly define what a "SCADA system" is, but most can agree that there are cooperative components that must work together to execute the functions associated with 'SCADA.' Tangibly, this will no doubt be different in each setting in terms of specific gear used to assemble and operate the systems functions, but taken together they are indeed "a" system. It would seem more appropriate to instruct identification of groups of cooperative components that work together to be treated as a system, and extraneous or stand alone or single-purpose equipment could be distinctly characterized as "unitary systems" when appropriate. There is practical value in logically treating several cooperative components as a system, and requirements for implementation documentation will be more straightforward and simpler if they can be treated as such. B) The fundamental flaw in the combined logic of CIP-010-1 (and transitively CIP-011-1) is the notion that risk to reliable operation of the BES posed by use of cyber assets correlates exclusively with the size of the electric operating site at issue. This single-minded orientation ignores other highly salient cyber security threat vectors in play,

#	Organization	Yes or No	Question 8 Comment
			most notably, concerning what type of data communications technology is used to network within and between sites comprising a BES Cyber System. The CIP V1 SDT correctly recognized the especial vulnerabilities posed by use of routable protocols, if the BES Cyber System is not secured with proper cyber security procedural controls and technical countermeasures. At the same time, less vulnerable - in terms of adverse impact on reliable operation of the bulk electric system as a whole - BES Cyber Systems or Components thereof that communicate using legacy serial, dial-up, or other Data Link Layer data transmission paths pose less of a practical risk in terms of overall BES attack surface due to their inherent lack of an Inter-Network Layer. Absent routable protocols, miscreant cyber navigation to and attack of other systems or components not directly attached to the individual serial link (dial-up or hard line) or Data Link Layer (sub-)network is simply not possible. Furthermore, the binary orientation of applicability of a requirement discussed above actually creates unsavory unintended consequences: in a number of ways a single requirement can mandate unnecessary and costly countermeasures for sites of a certain size regardless of the attack surface presented by the communications medium. That is, rigorous requirements appropriate for BES Cyber Systems/Components at sites that employ routable protocols are also imposed on other sites that do not, e.g., operating sites where only legacy serial lines are used. Finally, requirements for BES Cyber Systems/Components at work in purportedly small-impact grid operating sites where routable protocols are employed are in many cases simply deemed to be not applicable (not required). Summarily, the use of "electrical rating" (size) as the sole determinant of applicability of cyber security requirements will result in both excessive expenditures and undue regulatory risk concerning sites that pose minimal risk of cyber attack. This approach simultaneously fails to apply the Requirements to sites that, while not significant from an electric reliability standpoint, could afford a cyber entry point which could be used to access the larger network via routable protocols. Please see comments under Question 54 for a continuation of the above train of thought for explicit recommendations for improvements concerning both the structural organization and logical substance of CIP-010-1 and CIP-011-1 when taken together.

#	Organization	Yes or No	Question 8 Comment
8.4	Allegheny Power		Allegheny Power does not believe it is necessary to abandon the Critical Asset approach described in CIP-002. The new impact categorization structure proposed by CIP-010 introduces a completely new approach. All of the investment in procedures, training, documentation and other efforts to date to ensure compliance with the CIP standards will need to be redone. AP believes that the objectives of the Standard Drafting Team to provide further clarification and remove the uncertainty of the current CIP-002 are proper and necessary. However, AP believes that these same objectives can be accomplished by incrementally revising the current CIP-002 standard and not abandoning the approach entirely, which would essentially force all entities to start their CIP compliance efforts over from the beginning. Changing the terms, concepts and numbering schemes alone will disrupt continuity of CIP programs and have a major impact on each entity. Not all BES Cyber System components (as defined by CIP-010) face the same risk, or if compromised, have the same potential impact on the BES. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.5	Green Country Energy		An overall guidance document would be very helpful to the large number of entities that will have to comply with this standard that previously were not critical. Nothing specific, some reference links, examples of expectations, a resource guide.
8.6	CWLP Electric Transmission, Distribution		Any terms used, such as Operational Time Horizon, should be included in the NERC Glossary of Terms.

#	Organization	Yes or No	Question 8 Comment
	and Operations Department		
8.7	Dominion Resources Services, Inc.		Attachment II contains some errors and should be revised in accordance with the following; CIP-010-1 1.3. The term Wide Area is applicable only to a RC area. GOs do not have access to information necessary to make such a designation. This requirement should state that a RC must inform a GO within a certain specified time frame if the RC determines that the GO owns a "must run" unit. Also. there must be some "implementation period" for the GO to become compliant. Compliance may require extensive engineering, procurement and the expenditure of significant resources that must be considered when determining the appropriate implementation period. CIP-010-1 2.3. It is not clear which entities (e.g., BA, RC, TOP, other) have the responsibility to make such designation. GOs do not have access to information necessary to make such designation. The entities that have access to the information include the RC, TOP and possibly the BA. The RC should make the designation, but with the input of the BA and TOP. If the RC makes such a designation, it is proposed that this requirement be revised to contain a statement that the RC must inform the GO within a certain specified time frame. Also, there must be some "implementation period" for GO to become compliant. Compliance may require extensive engineering, procurement and the expenditure of significant resources that must be considered when determining the appropriate implementation period. NOTE - Currently, in PJM, units so designated do not impact the entire RTO (equivalent of Wide Area) but are designated due to local import constraint limits (CETL). It appears likely that such generator would be designated as Medium impact. However, in smaller RC areas (e.g., NY), this could result in generators that appear to be equal in size (to a generator designated as medium in PJM) being designated as High because the impact to that RC area is based on size of the area as well as the generators within that area.

#	Organization	Yes or No	Question 8 Comment
8.8	Constellation Energy Commodities Group Inc.		Based on the current CMEP the audit cycle will always be longer than a full calendar year, would it be clearer to state that the data retention period is for 3 years.
8.9	Constellation Energy Control and Dispatch, LLC		Based on the current CMEP the audit cycle will always be longer than a full calendar year, would it be clearer to state that the data retention period is for 3 years.
8.10	ReliabilityFirst Staff		Because the acronym "BES" is not included in the NERC Glossary of Terms, we suggest that BES should be spelled out in the Introduction to this standard.
8.11	Reliability & Compliance Group		Being more specific with better definitions is a tremendous help with interpreting the requirements. Right now, there is still too much open to interpretation and as such, this will be very hard to make auditably compliant anywhere but to our own procedures.
8.12	City Utilities of Springfield, Missouri		City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
8.13	IRC Standards Review Committee		Comments: NERC should lead a discussion of whether the proposed CIP standards provide an appropriate level of protection from attacks. By level, we mean the granularity of the requirements - or how far down to individual components and personnel procedures. Attempting to put requirements to protect from nearly every possible attack scenario possible on every possible asset and or component that touches the BES is an extraordinary effort that will certainly provide a perception that NERC and the registered entities are doing what they can to protect from threats. There is no argument that if every registered entity protects every asset/component from threats to the nth level of granularity, the industry would be able to state that it has made every possible effort to thwart attempts to sabotage the interconnected grid. But NERC should begin a discussion on whether it is necessary to have such extensive requirements to be able to prevent a system-wide incident. The proposed CIP standards do not seem to align with NERC's approach in setting reliability requirements for more "traditional" system threats such as facility loading and system frequency. With these "traditional" standards, there is a distinction between requirements and procedures that are local in

#	Organization	Yes or No	Question 8 Comment
			nature and those that are needed on a wider interconnection level. For these "traditional" reliability threats, it is accepted by industry and regulators that this is an appropriate approach. For example, NERC does not establish requirements for relay maintenance crews to properly disengage trip coils when testing relays. But NERC does establish standards for registered entities to maintain those relays that impact BES reliability. The details of how the registered entity ensures that maintenance programs are carried out requires a local or individual procedure/requirement. NERC's focus should remain on setting standards to protect from wide area impacts - not on establishing standards that manage individual system components. NERC and the industry need to take a hard look at what exactly the CIP standards should protect from and write standards that can leverage compliance resources to reducing the wider interconnection level threats and leave setting measures or requirements that are local in nature up to the registered entities.
8.14	Southwest Power Pool Regional Entity		Consider combining the Medium and Low categories into a single category. A three tier categorization is not necessary.
8.15	Public Service Enterprise Group companies		Considerable effort was spent by industry stakeholders in classifying assets as Critical Assets (CAs) and as Critical Cyber Assets (CCAs) for CIP v1-v3. An official guide to map identified assets using the CIP v1-v3 CA and CCA terms and the new BES Cyber System Component and BES Cyber System terms is needed. Such will be an aid in ensuring a smooth transition.
8.16	Oncor Electric Delivery LLC		Control Centers and substation need to be considered separately. What is prudent cyber protection at a control center may be totally unnecessary at a substation.
8.17	E.ON U.S.		cyber systems used exclusively for local distribution of electric energy is contrary to FPA Section 215 (1) & (3). Other comments on specific areas of the proposed standards: CIP-010-1 B Requirements Section 3.2,3.3 What constitutes a "change" under these requirements.

#	Organization	Yes or No	Question 8 Comment
			CIP-010-1 C. Measures, M3 E.ON U.S. requests that the SDT clearly define in which requirements this measure applies. CIP-010-1, Violation Severity Levels There is very little difference in risk between failing to update documentation for 60 versus 80 calendar days, yet there are various gradations based on the 10-15 day window from the low-to-severe. CIP-010-1, section 3 "Low Impact Ratings" Maintaining an inventory of all low-impact rated BES cyber systems/ components will result in a significant administrative burden. Given the few prescribed protective measures that apply under CIP-011 to low impact facilities the inclusion of low impact facilities appears to provide little in the way of additional BES reliability.
8.18	San Diego Gas and Electric Co.		Draft Standard CIP-010-1 is a significant paradigm shift from the currently effective Standard CIP-002-2. SDG&E has spent significant resources to be compliant with the current version of the CIP Standards including becoming knowledgeable with the current terminology and applying it within the current CIP Standards. Draft Standard CIP-010-1 departs from the current CIP Standards but at the end of the process, it is unclear whether this change in approach will in fact result in a material enhancement to the reliability of the BES. SDG&E suggests that before continuing to move forward, the SDT needs to specifically understand and communicate to the industry what it is trying to accomplish. What is the target that we are all trying to hit with these proposed changes to the CIP Standards? In so doing, the industry can provide specific alternatives that accomplish the goal at hand. When evaluating the alternatives to meet the goal, it is critical that there is a quantifiable incremental reliability benefit to the BES before proceeding. SDG&E and many other entities have spent significant resources to comply with the current CIP Standards. At this point in time, the industry needs to know that additional resources to

#	Organization	Yes or No	Question 8 Comment
			comply with the proposed CIP Standards will result in an incremental benefit to the reliability of the BES. SDG&E strongly recommends that before moving any further, these questions be answered and that the SDT actually "test" the proposed draft CIP-010-1 Standard on a handful of companies or scenarios to gain some practical experience from the proposed changes. Are the in-scope assets easy to identify and categorize? How does the quantity of in-scope assets compare to that of the current Standards? Perhaps the SDT will find that there is a significant enhanced reliability impact to the BES. On the other hand, the SDT may find that the results do not accomplish the goal that it is trying to achieve and thus another approach would make more sense. SDG&E advocates leveraging the existing CIP Standards as much as possible moving forward, because we (like many others) have a lot of time and resources invested in our current compliance efforts and we'd really like to build from those efforts instead of essentially starting over with a new process.
8.19	BCTC		Emergency Situations - The provision for "emergency situations" should remain at the policy level. BCTC is of the opinion that it is feasible for emergency situations to be unforeseen and, as such, does not agree with the assigning of such contingencies to specific requirements.<See CIP-011-1-R3 below for an example> TFEs - TFEs will continue to be required due to the limitations of technology - i.e. older systems being unable to enforce strong passwords, etc. These limitations are beyond the Utilities control and, as such, it would be considered unfair to be found in non-compliance for such instances. What should be required in such situations is that the Utility implement controls to minimize the vulnerability that results from the TFE.
8.20	Exelon Corporation		Exelon companies have embraced the development of logical, clear and effective reliability standards as evidenced by its commitment of time and resources to various standard development initiatives (including participation on several NERC and Regional Committees, Sub-Committees and Standard Drafting Teams). As evidence of our

#	Organization	Yes or No	Question 8 Comment
			commitment, Exelon has devoted in excess of 4 years and $11 million for the implementation and integration of the NERC CIP-002 to CIP-009 Standards. We have concerns with several aspects of the CIP Version 4 Standards. The CIP Version 4 Standards represent a significant change in the scope of the standards in the equipment/systems that fall under the standards as well as the elimination of terms/categories of assets. Exelon is also not in favor of changing the current CIP-002-009 standards to the new CIP-010 and CIP-011 format. Each change in itself represents a significant "change management" issue that impact databases used for the tracking/storing of evidence of compliance, training requirements, safeguards, and systems that have been put into place to ensure Exelon's continued compliance to all NERC Standards. Exelon feels strongly that the proposed changes must be accompanied by a risk based analysis as justification for such dramatic and costly changes which to date have not been shared with the industry. Essentially we are most interested in understanding the incremental difference or benefit of moving away from the current Regulatory approved CIP-002 to CIP-009 standards to a different set of standards that will result in many of us "starting from square one" to implement. If this shift to CIP-010 and CIP-011 is approved, policies, procedures, contracts, training, drawings, methodologies, systems, data structures, and countless other documents will need to change to reflect the new language and concepts. The confusion that this will cause within organizations to retrain personnel and realign around the new standards cannot be underestimated. In fact, Exelon may even need to put some value-added compliance projects on-hold because the entire design will need to change with the implementation of the new standards. Specifically, Exelon would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- but use the standards drafting team work as an input to the process. Incrementally change the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable

#	Organization	Yes or No	Question 8 Comment
			continuity. This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure.
8.21	Duke Energy		Explicitly state that terms found in the NERC glossary apply here unless otherwise stated.
8.22	USACE - Omaha Anchor		General comment - committee referred to relays as being addressed in this standard. We are unsure what that interpretation is based in attachment 1.
8.23	Powersouth Energy Cooperative		General Comments: The approach to classify cyber systems according to their impact seems to be a better approach for the industry. Taken in conjunction with CIP-011 that establishes security requirements, it is logical to establish security levels based upon the impact of compromising these assets. The drafting team is commended for this approach. Consideration should be given however to recognizing that while technically some assets are BES assets, they do not materially affect the BES. For example, a small DP may own UFLS relaying however the magnitude of the load that is shed by their entire UFLS program would insignificantly affect the overall objective of the regional UFLS programs to protect the BES. While identifying those assets is reasonable, to require any security measures in CIP-011 is not warranted. Perhaps a "No Material Impact" category should be considered based on load. R1. There is a perception that every cyber system associated with the BES owned by an entity must be identified to determine if the cyber system executes or enables one of the functions in the attachments. It would seem appropriate to review all facilities (i.e. locations) to determine and document the functions that are performed at that location. However, if it is determine that no BES functions are performed documenting each system seems to provide little benefit. Example: A small distribution station is served from a transmission line greater than 100 kV. The station does have multiple cyber systems none of which perform identified BES function. The perception is each system must be documented. Since on a higher level,

#	Organization	Yes or No	Question 8 Comment
			a functional assessment indicated no BES functions are performed, is it necessary to document each cyber asset?
8.24	American Municipal Power		I agree with the intent, but I disagree with the structure of CIP-010. The applicability section should not include Distribution Providers (DP), since many DP will have little to no impact to the reliability of the BES from a cyber standpoint and will have to comply with many burdensome and unnecessary requirements in CIP-010 and CIP-011 that will be performed by other entities. I feel the purpose of the standard should directly relate to an increase in reliability. I feel the CIP-010 standard is solely based upon documenting existing or planned systems, so the purpose should correlate documenting the cyber systems with an increase in reliability. There should only be two requirements. R1: Document BES Cyber Systems. R2: Review documented BES Cyber Systems. Please add sub-requirements only as necessary to fulfill the purpose.
8.25	Matrikon Inc.		I offer to provide a workflow decision diagram I have prepared (Visio or JPG) to show how CIP-010 could be interpreted, but also to see how each of the statements in the requirement are supposed to fit into evaluation of BES Cyber Systems. I am a visual person, and my goal was to visualize the interpretation of CIP-010 for myself and colleagues to have a clearer understanding of its application. Diagram has been sent directly to Lauren.Koller@nerc.net as part of my comments. Use at your discretion, feel free to leverage/expand on my diagram, and share with SDT. My intent is to simply help reduce misinterpretation of the standards and debate on how they should be applied.
8.26	Cogeneration Association of California and Energy Producers & Users Coalition		Is it the intent of the Drafting Team that a cyber system will not be classified as a BES Cyber System if it does not cause a disturbance to the BES within 15 minutes or does not have an effect on real-time operation of the BES within 15 minutes of it becoming unavailable, degraded, compromised, or misused? If yes, guidance will be needed on

#	Organization	Yes or No	Question 8 Comment
			what proof of lack of disturbance is necessary to support an entity not classifying a cyber system as a BES Cyber System.
8.27	EEI		It would be helpful for the drafting team to develop in a separate guidance document more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES. Over the last several years, a number of parties have expressed concern about the risk associated with multiple, simultaneous remote attacks against BES Cyber Systems, potentially impacting multiple generation, transmission and control center facilities. If in fact, the primary concern is the issue of multiple, simultaneous remote attacks, it is not appropriate to mandate excessive controls over physical elements such as the copper or fiber optics cable plant within a generating facility or a building housing a control center. Security requirements and controls should be developed that are proportional to the potential or probability of compromise as well as impact of compromise.EEI suggests that the drafting team recognize that not all BES Cyber System components face the same risk based on their connectivity. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.28	ISO New England Inc		Modify the purpose statement to be more clear and understandable. Proposed Purpose: To identify and categorize BES Cyber Systems that execute or enable

#	Organization	Yes or No	Question 8 Comment
			functions essential to reliable operation of the BES. Apply appropriate cyber security requirements commensurate with the adverse impact that loss, compromise or misuse of those BES Cyber Systems could have on the reliability of the BES.
8.29	Hydro One		Most North American utilities spent significant capital and manpower resources in order to achieve compliance with current version of CIP standards. Version 4 brings a multitude of changes that appear to significantly broaden compliance requirements. Hydro One understands and supports the intent to improve the overall reliability of the BES through reduction of the vulnerability to cyber attacks. Based on the previous experience, in the development of the version 4 implementation plan, the SDT should consider the long time periods necessary to implements the changes required for this version.
8.30	Michigan Public Power Agency		MPPA is concerned with how these standards would impact its members who are registered entities but do not own or operate facilities that are, by NERC definition, a part of the BES. MPPA recommends clarification in the applicability section with the insertion of ", that operates BES facilities, " between "...Functional Entities..." and "...will be collectively...". This segment of the sentence would then read as: "...Functional Entities, that operates BES facilities, will be collectively..."
8.31	MidAmerican Energy Company		Need to ensure the VSLs are not written with zero-defect quality prescriptions. The proposed VSL levels in CIP-010 are too prescriptive. Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: o program implemented o program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) o correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity

#	Organization	Yes or No	Question 8 Comment
			levels should correspond, for example: VSL For Severe program not implemented High controls not implemented Moderate reviews not completed Lower corrections from reviews not completed These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
8.32	Progress Energy - Nuclear Generation		NERC should facilitate the Federal Energy Regulatory Commission (FERC) consideration to suspend implementation of Critical Infrastructure Protection (CIP) Reliability Standards CIP 002 through 009 for nuclear plants in favor of implementing CIP-010-1 and CIP-011-1. Originally, CIP-002 through 009, Version 4, were to be developed to address nuclear cyber requirements as a result of FERC Order 706-B. However, CIP-010-1 and CIP 011-1 are now being developed to address the nuclear cyber requirements. In the mean time, nuclear will be required to implement CIP-002 through 009, Version 3, which do not align with CIP-010-1 and CIP-011-1 to satisfy the FERC requirements. CIP-010-1 and CIP-011-1 could be implemented at the nuclear plants in the same time frame licensees committed to the Nuclear Regulatory Commission for the 10 CFR 73.54 required Cyber Security Plans. Using the current North American Electric Reliability Corporation (NERC) timeline approved by FERC, R+18 of CIP 002 through 009, Version 3, (~ August 2011), the timing of implementation of CIP-010-1 and CIP-011-1 will be well after CIP 002 through 009 and potentially 73.54. This will require multiple reiterations of nuclear licensee cyber security plans and implementing programs and procedures. These changing requirements create potential error opportunities.
8.33	NextEra Energy Corporate		NextEra suggests a re-write of the following provisions as set forth below to provide

#	Organization	Yes or No	Question 8 Comment
	Compliance		clarity: 4.2. Physical Facilities 4.2.1. All BES Facilities under NERC jurisdiction, including those nuclear generating plant facilities that as part of FERC Order 706-B (and other applicable FERC orders) processes are determined to be subject to this CIP Standard. B. Requirements R1. For each BSE Control Center, Generation Facility or Transmission Facility implicated by the Responsible Entity's application of High, Medium and Low Impact Risk in Attachment II to its BES, the Responsible Entity shall identify and document all BES Cyber System Components that it owns and indicate its association with a BES Cyber System. (Violation Risk Factor: High) R2. The Responsible Entity shall ensure that each BES Cyber System Component identified in R1 is in compliance with the applicable protections as required in CIP-011-1. (Violation Risk Factor: High) CIP-010-1 - Attachment I (For informational purposes only) Functions Essential to Reliable Operation of the Bulk Electric System The following provides an understanding of the operating functions which are essential to real-time reliable operation of the BES and are provided for informational purposes only.
8.34	Independent Electricity System Operator		No, but please see our comments under Q9.
8.35	USACE HQ		Please answer to questions 3 and 4.
8.36	FirstEnergy Corporation		Please see Question 1 for FE's Summary view on the CIP-010 and CIP-011 standard.

#	Organization	Yes or No	Question 8 Comment
8.37	BGE		Provide a definition for “Automatic Load Shedding”.
8.38	Puget Sound Energy		Puget Sound Energy notes that the Violation Severity Levels put specific metrics (5%, 10%, etc...) to previously commented on vague terminology. In order for NERC to determine “5% or fewer BES Cyber Systems have not been identified”, there has to be a total number of BES Cyber Systems at an entity. But, with vague, open to interpretation, terms like “restrict” or “affect”, the total list of BES Cyber Systems is subjective to different opinions on what it means to restrict or affect the BES.
8.39	Liberty Electric Power, LLC		RE: VSLs. Smaller facilities with limited cyber assets will pay a much larger penalty for a single miscategorized asset than a large utility. Example: TOP miscategorizes 49 of its 1000 cyber assets, and gets hit with a single lower VSL. Small generator miscategorizes 1 of 8 cyber assets, gets hit with a severe violation. Some method of recognizing the disproportionate affect on smaller entities must be included in the standard.
8.40	LCEC		Recommend that the development and release of implementation guidelines takes place sooner rather than later to assist entities in complying with the new standards.
8.41	Minnesota Power		Regarding the Violation Severity Levels, how does the Standards Drafting Team envision these being applied? If systems are not identified, how will an auditor know how many are missing? For example, VSL R2 mentions “incorrectly categorized” BES Cyber Systems. How will an auditor determine that a Registered Entity has incorrectly categorized systems when they have documented their review and categorization process? Also, for VSL R3, it seems arbitrary that a difference of 20 days takes a violation from a “Lower” to a “Severe” VSL. How were those numbers determined?
8.42	Wolverine Power		See comments listed for 1.a
8.43	Nuclear Energy Institute		Several:

#	Organization	Yes or No	Question 8 Comment
			a) In the Introduction, Section 3 (A.3), the word "could" should be replaced with "would." b) In the Introduction, Section 5: Clarification should be made that upon approval by FERC, CIP 010-1 supersedes, in their entirety, all prior versions of the CIP standards, and that compliance with the requirements of CIP-010-1 must be in accordance with the implementation schedule for CIP-010-1.
8.44	APPA Task Force		The APPA Task Force commends the drafting team on their work on CIP-010-1. We thank the team for its hard work and appreciate the team's consideration of our comments from the previous informal comment period. We think the standard is moving in the right direction and with this next round of comments should hopefully result in a set of standards that will meaningfully improve the reliability of the BES and address the cyber security issue for the industry.
8.45	US Bureau of Reclamation		The changes in the Standards to focus on Cyber Systems is reasonable, but the definitions for Cyber System Components, Cyber Systems, and Control Centers may need further refinement (or application examples) to help implementation staff address fundamental questions. As an example: Is an isolated electronic relay providing generator protection for a single large generation resource a BES Cyber System? Under the present definitions it would appear to be (it certainly qualifies as a BES Cyber System Component). If it is a BES Cyber System, it is subject the requirements of CIP-011 based on the impact of the "System." Is this really the intent of the drafting team(s)? Would it not be better to establish select security criteria for isolated components (specifically components such as cyber-based relays and synchronizing equipment) that fit the nature of their deployment - rather than trying to fit them into a "system" category?
8.46	Southern California Edison Company		The CIP-010 and CIP-011 drafts should indicate how these standards will replace or supplement the current CIP-002 through CIP-009. If the intent is to retire CIP-002 through CIP-009 then it would make more sense to call these standards CIP-002-5 and CIP-003-5 with CIP-004 through CIP-009 being retired. A gap of unused numbers

#	Organization	Yes or No	Question 8 Comment
			between CIP-001 and CIP-010 will potentially cause future confusion.SCE also requests the Standards Drafting Team clearly define what should be included as Protective Systems. Additionally, a matrix mapping CIP Version 3 requirements to CIP Version 4 requirements would be very helpful.
8.47	LADWP		The CIPs should evolve in a manner that does not minimize the investment of resources already expended to meet compliance but should leverage the work done already. The draft version 4 is a drastic change and would require multiple years for a Responsible Entity to approach compliance. If CIP version 4 is implemented as currently drafted, there would be a huge resource drain to rewrite language and requirement references that are now part of numerous policy and procedures as well as contract packages.
8.48	Xcel Energy		The definition of BES Cyber System uses criteria that the element must be capable of causing a system disturbance or other impact within 15 minutes. We would like to know if or classification based on the 15 minutes must rely on analysis or if judgment/expert opinion is allowed. 1.5 Please clarify that the “Texas Interconnection” refers to ERCOT. 1.5 If a cyber system can only impact 1 transmission line within a substation containing 4 or more lines, it should not be classified as high. Suggest 1.5 wording be changed to Each BES Cyber system that can affect operations for: “Four or more Transmission lines operated at 300 kV or higher in the Eastern and Western Interconnections or operated at 200 kV or higher located at Transmission Facilities within the Texas and Quebec Interconnections 1.9 It is not clear why facilities serving a nuclear site under NUC-001 are high impact if the nuclear site itself is not High impact.
8.49	Dairyland Power Cooperative		The distinctions between systems and facilities are unclear. The Requirements in CIP-010 shift to a systems oriented identification. Yet the Attachment I/II definitions still rely

#	Organization	Yes or No	Question 8 Comment
			on the concept of facilities and almost seem to equate facilities with systems. These distinctions need to be clear.
8.50	Con Edison of New York		The Drafting Team needs to take into account the fact that the ability to work on any cyber systems in a substation will typically already require a detailed work permit process which includes getting a work permit from an operating authority with jurisdiction on the equipment. The employee working on the cyber system must typically be an approved employee to work on these systems.
8.51	FEUS		The drafting team should consider an alternative for the VSL categorization. By basing it on a percentage, it could potentially unfairly affect smaller entities with fewer BES Cyber Systems. A smaller entity will inherently have fewer BES Cyber Systems, so missing a single classification of a BES Cyber System could automatically merit a severe violation. For example, an entity with as few as 5 BES Cyber Systems that misses the identification of a single system would be in a severe category. A larger entity with inherently more BES Cyber Systems can fail to identify more BES Cyber Systems and have a lesser severity level. An entity with 50 BES Cyber Systems can fail to identify 8 before reaching a severe violation level. The risk of failing to identify 8 BES Cyber Systems puts the BES at a much higher risk than failing to identify 1 BES Cyber System.
8.52	Indeck Energy Services, Inc		The FERC directed guidelines to Registered Entities on the risk based assessment methodology are missing.
8.53	PacifiCorp		The low, moderate and high violation severity levels for R3 do not seem to measure the correct violation criteria. The number of days after a change is completed should not be the sole criteria. The number of days after a change is completed should not be the sole criteria for determining whether a violation was harmless or severe. This is especially true for a standard that currently has no meaningful qualifier to allow for routine or de - minimus changes to elements of the BES without triggering a full review. These criteria should track other violation criteria that consider whether the violator had an adequate

#	Organization	Yes or No	Question 8 Comment
			process in place for the types of changes that merit a re-evaluation. Need to ensure the VSLs are not written with zero-defect quality prescriptions. The proposed VSL levels in CIP-010 are too perscriptiveprescriptive. Replace zero-based quality prescriptions in the requirements, measures and violation severity levels with based performance targets that correspond to the vulnerability of concerted, well-planned attacks against multiple points. For example, requirements and measures should focus on performance objectives as follows: o program implemented o program and security controls in place reviewed periodically (for example, every 12 months not to exceed 15 or every 90 days not to exceed 120) o correcting items found in the reviews timely (for example, within 30 days not to exceed 45). When an entity consistently performs, the security control objectives will be achieved. Violation severity levels should correspond, for example: VSL For Severe program not implemented High controls not implemented Moderate reviews not completed Lower corrections from reviews not completed These should replace zero-defect quality prescriptions as perfection is not essential to achieving the objective of vastly reducing the risk of concerted, well-planned attacks against multiple points.
8.54	National Rural Electric Cooperative Association (NRECA)		The Purpose section of CIP-010-1 and CIP-011-1 should be similar in regards to the facilities it refers to. Add the word in all CAPS to the CIP-010-1 Purpose to bring it in line with the Purpose in CIP-011-1:".... that execute or enable functions essential to reliable operation of the INTERCONNECTED BES..."
8.55	SCE&G		The SDT needs to consider how auditors may interpret the words of the standard

#	Organization	Yes or No	Question 8 Comment
			differently. The language needs to be written clearly and concisely enough so that a consistent interpretation of the standard will be applied by all auditors across all regions. Consideration of Nuclear Facilities: Definitions for BES Cyber System and BES Cyber System Component conflict with definitions that have been accepted by the Nuclear Regulatory Commission (NRC) in NEI 08-09 Revision 6 for Critical System and Critical Digital Asset; recommend for nuclear systems subject Federal Energy Regulatory Commission (FERC) 706-b definitions for FERC and NRC regulated systems are consistent. This will avoid regulatory uncertainty as well as human error at nuclear facilities. CIP-010-1 R2 and Attachment 1 - some of these functions are covered by NRC regulation. Will issuance of this document require re-submittal of systems for exemption after the Bright Line submittal of systems? The implementation schedule for CIP 10 - 11 versus CIPs 02-09 requires doing the same reviews twice and is an unnecessary burden on nuclear licensees as well as other FERC critical assets. The deterministic nature of the security controls in CIP 11 do not provide for acceptance of Common Controls as defined by NIST 800-53. In nuclear facilities with mature physical security programs, engineering control programs, and physical segregation of trusted industrial control system networks from un-trusted networks, CIP 11 should include provision for NIST 800-53 Common Control processes.
8.56	Consultant		There appears to be inconsistency in use of terminology throughout the standard as the terms apply to defined glossary terms, new definitions contained in this standard, and what appear to be 'common terminology' that is not defined. The terminology should be reviewed and applied consistently to avoid ambiguity and confusion. It is not clear that the implied process in the requirements (R1. Identify BES Cyber Systems, R2. Categorize Cyber Systems) is the best methodology. This seems to be missing the first step of the process: 1. Identify the BES assets (Facilities, Elements, &

#	Organization	Yes or No	Question 8 Comment
			Control Centers). The previous versions of CIP-002 started with the identification of BES assets followed by inclusion or exclusion as Critical Assets using the Risk-Based Methodology. As the current standard is written it seems to have lost the step to identify BES assets to which the CIP-010 R1 & R2 steps would be applied. Suggest adding the 'first step' to identify BES assets. This would probably require some restructuring of the current R1 & R2 statements to apply them to the identified BES assets.
8.57	Ameren		There are no system performance requirements as part of the determination of “High”, “Medium”, or “Low” impact to the BES other than item 1.7. The addition of performance requirements from the TPL standards (TPL-003 and 004) could further help to identify which facilities have the biggest impact on the BES and reduce the number of “High” and “Medium” impact facilities identified to provide significant cost savings to the industry.
8.58	WECC		Utilizing the prescriptive nature of CIP-010-1 Attachment II would be very useful as a rewrite of CIP-002-4. The CIP-002 through CIP-009 format lends itself very well to being audited. What is needed is clarification and explicit language. The current standard needs to be made better not replaced.
8.59	Kansas City Power & Light		Very concerned regarding the “lines” that have been drawn in Attachment II. What is the engineering basis for any of the “bright line” thresholds that have been expressed in Attachment II? Recommend thoughtful consideration regarding operating assumptions be developed an analysis be performed to establish the facilities that should be considered HIGH, MEDIUM and LOW reliability impact. Operating criteria should be established to determine what has HIGH, MEDIUM and LOW reliability impact. In addition, there are facilities that have NO IMPACT to reliability of the BES. Whatever criteria is established, a “smell test” should be done to see if the criteria works. There are numerous small Regional Entities that are obviously no impact to the reliability of the BES, and if any of these requirements and definitions draw any of the facilities of these small entities into the CIP Standards, something is wrong and adjustment to the criteria

#	Organization	Yes or No	Question 8 Comment
			needs to be considered.
8.60	ERCOT ISO		Violation Severity Levels: Recommend that VSLs address “identify” and “document” BES Cyber Systems. “Identify” and “document” are noted separately in the requirements. Attachment I: What is the originating source for this? Can it be referenced? What does “BES elements” mean?
8.61	Pepco Holdings, Inc. - Affiliates		We agree with EEI’s comments regarding not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES (e.g. serially attached electronic components versus those that use routable protocols; devices that communicate to each other within a self-contained, isolated network segment versus devices that communicate via routable protocols across multiple geographic or logical boundaries, and devices that use dedicated (and non-routable) point-to-point communications channels versus devices that communicate via routable protocols across multiple geographic or logical boundaries). Would suggest that consideration be given up front in CIP-010 to the types of communication/risk when developing security requirements.
8.62	We Energies		We Energies agrees with EEI. It would be helpful for the drafting team to develop additional documentation providing more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES. Over the last several years, a number of parties have expressed concern about the risk associated with multiple, simultaneous remote attacks against BES Cyber Systems, potentially impacting multiple generation, transmission and control center facilities. If in fact, the primary concern is the issue of multiple, simultaneous remote attacks, it is not appropriate to mandate excessive controls over physical elements such as the copper or fiber optics cable plant within a generating facility or a building housing a control center. Security requirements and controls should be developed that are proportional to the potential or probability of compromise as well as impact of

#	Organization	Yes or No	Question 8 Comment
			compromise. Not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES. o Serially attached electronic components do not face or create the same risk as those that use routable protocols. o Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries. o Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
8.63	Progress Energy (non-Nuclear)		We need definition of when the CIP requirements "turn on" during new plant construction, commissioning, and/or start-up. Recent major projects with CIP CCA's have been add-ons to existing facilities. We have used the model that until we "logically" connect to the existing facility ESP the full CIP requirements were not required. The next projects will be new facilities with no ESP logical connection to the existing steam plants. We should recommend wording that states that the CIP ESP and PSP requirements do not turn on until the plant is turned over to Energy Supply for commercial operation and it becomes available to ECC. Argument being that during testing ECC manages other generation assets to allow for testing impact on BES. Standard malware protection rules (A/V, etc.) would still apply. Have the regional entities auditing & compliance groups made an initial assessment as to the relative impact when compared to existing standards? For example do they anticipate significant increase in compliance records and audit evidence required? Unofficial Comment Form - CIP-010-1 and CIP-011-1 Cyber Security Order 706 (Project 2008-06)

#	Organization	Yes or No	Question 8 Comment
			Is there expected to be a TFE process for these standards - based on current experience the TFE process is more onerous and adds considerable paperwork without effectively enhancing security of BES. Need consideration for redundancy, backups, alternate systems in relation to required levels of protection - CIP-010-1 R1 makes no provision for considering redundancy, backup systems, or alternate systems which may be in place to 'provide assurance in the resiliency of these functions.' But according to the NERC document Guidance for the Electric Sector: Categorizing Cyber Systems, providing for the 'assurance in the resiliency of these functions' is part of 'The Purpose of Categorizing BES Cyber Systems'. Failure to consider these additional systems as layered safeguards and thereby reducing the criticality of any one of them may mandate that each such BES Cyber System be considered equally essential and critical. The result would be to provide disincentives for the responsible Entities to implement these additional layers - reducing the assurance in the resiliency of these functions. This would be contrary to the stated purpose of 'reducing risk to the performance of functions.' Need better provision for standards tailored to various asset types - Although the new standards will bring even more 'single use' equipment into focus, the standards are designed to protect 'multi function' PC based equipment from the attack vectors that they present. The standards need to take into consideration equipment that doesn't require protection (or extra work such as a TFE) for vulnerabilities that do not exist. Example: A terminal server which is a 'single use' type platform that only does protocol conversion between serial and Ethernet communications presents very few attack vectors. The same functions could be performed by a fully functional PC but that device would present a much larger opportunity for a hacker. The current version of the standards will actually make it more advantageous for entities to implement this function using the larger target of a fully functional PC rather the 'single use' type device simply because of ease of compliance. Recommend implementation timeline:

#	Organization	Yes or No	Question 8 Comment
			High - 4 years Medium - 4 years Low - 4 years
8.64	US Army Corps of Engineers		Will there be official guidance documents, such as the DRAFT Guidance for the Electric Sector: Categorizing Cyber Systems?
8.65	Verizon Business		1. It is not clear whether electricity trading was considered in the draft standard. 2. Attachment III Section 1.11 discusses "BES Elements that perform automatic aggregate load shedding of 300 MW or more." This statement should be revised to specifically exclude Smart Grid Distribution. 3. This standard should be compared to the elements included in the NERC Frequently Asked Questions for CIP-002 to ensure that any new and different perspectives from the FAQs woven into the CIP-002-4 version are addressed completely. 4. The inclusion or exclusion of "non-routable protocols" under CIP-002-4 needs to be addressed. For instance, if the standard included all protocols, then a substantial number of communications systems (e.g., Serial, SONET, etc.) would now be included in the list of "BES Cyber Systems." This would be a substantial change to the Registered Entities, and compliance would be difficult. Overall, non-routable protocols should be included in the CIPs as well as routable protocols. 5. An explanation is required for the inclusion of Distribution Provider in Section 4, Applicability. The inclusion herein has caused confusion for Smart Grid implementation. The Distribution Provider should not be included. 6. In the BES Cyber System Component definition, the word "Disturbance" is capitalized. This word should be defined in the Glossary and could be included as a

#	Organization	Yes or No	Question 8 Comment
			Local Definition in CIP-010. To assist implementing utilities, it would be useful to do some mapping and case studies of the transformation of “Critical Assets” and “Critical Cyber Assets” to “BES Cyber Systems” and “BES Cyber System Components.”

9. **Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference?**

Summary Consideration:

There was no clear preference from the compilation of responses received. Many entities liked the approach and structure provided by the posted CIP-010 and CIP-011, while a substantial number would prefer to keep the current CIP-002 – CIP-009 structure. Reasons provided by the latter centered around substantial compliance management frameworks implemented to support the CIP-002-CIP-009 structure. Others offered a hybrid approach, with some grouping.

The SDT has considered these comments and has opted to keep, in large part, the current structure of CIP-002 – CIP-009, with the addition of two new standards, CIP-010 and CIP-011. The two additional standards allow for some requirements from previous standards, where the subject matter did not quite fit, to be separated into the additional standards. In this manner, the SDT believes that each standard consists of a set of related requirements that support an identified purpose.

#	Organization	Yes or No	Question 9 Comment
9.1	WECC		This seems to be essentially a formatting issue. If the same requirements are included in either on single standard or multiple standards, the preference is with the individual reader. Keeping it as one single CIP-011-1 standard will ease discussions throughout organization when talking about CIP as there will only be one standard for all controls and it makes sense based on the previous versions repeated statement that the standards should be treated as one standard.Breaking CIP-011-1 into multiple standards lends itself very well to being audited. In either option, what is needed is clarification and explicit language. Regardless of the format, the standard (s) needs to be made stronger, more clear, more concise.
9.2	ISO New England Inc	Break CIP-011-1 up into multiple standards	- Disagree with the current structure- Establish new standards by functional areas- Ensure there is not a circular loop relating to other requirements/standards, each requirement/standard should be standalone

#	Organization	Yes or No	Question 9 Comment
9.3	IRC Standards Review Committee	Break CIP-011-1 up into multiple standards	(i) We disagree with the current structure. We'd suggest the SDT to establish new standards by functional areas and ensure there is not a circular loop relating to other standards. Each standard should be standalone(ii) We understand the need for this standard to take care of cyber security concern when there does not currently exist an across-the-board cyber protection standards that apply generically to all sectors that utilize cyber components and cyber access for control and data exchange. However, over time, we urge NERC and the electric industry to assess if indeed it needs to have its own cyber protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions. Wouldn't the electric industry be better served if owners of BES Cyber Systems be required to adopt similar practices of these other sectors as opposed to developing it own very detailed set of requirements which, for the most part, seem to replicate the other sectors' requirements?It will be desirable to have a generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems - may they be for BES control or access to airline reservation, air traffic control, e-banking, security trading, etc. NERC and the electric industry should take the lead to initiate a continent-wide effort to consolidate all such standards and practices to avoid redundant efforts.
9.4	Entergy	Break CIP-011-1 up into multiple standards	A) Compliance Enforcement Problems: From the point of view of both implementation and auditing of Requirements it makes little difference as to the granularity of Requirements contained per Standard. However, from an enforcement perspective, using a single Standard document consisting of many Requirements is highly problematic. Per the current codified NERC Standards Development Process any Standard can be assigned only a single Violation Risk Factor (VRF). Consequently, even if only one Requirement in the single document approach is considered a "High" Risk Factor, then the entire Standard must be designated as High. This is problematic first in that not all CIP Requirements contained in either CIP-003-3 through CIP-009-3 or CIP-011-1 are of equal salience in terms of security vulnerability/risk created in virtue of failure to comply - some are indeed High, but by no means all. [However, note that

#	Organization	Yes or No	Question 9 Comment
			determination of Violation Severity Level (VSL) is not especially problematic - it's still a measure of just 'how far out of compliance' the Entity is.] Second, it is hard to imagine any Responsible Entity being 100% compliant with every Requirement in a single large Standard in any calendar year; it could well be that all Responsible Entities in the industry are found to be out of compliance with some aspect of a single large multi-Requirement Standard every year. Statistically, this does not speak accurately as to the quality of the NERC Standard, its Reliability Standards Program, or the industry's attentiveness or sense of urgency concerning the need for proper cyber security. For the reasons above, Entergy submits that a larger number of Standards, with fewer, more finely focused Requirements in each will serve our collective purposes much better.B) Cost Impact: Moreover, the cost of revising all the existing procedures, database systems, and other compliance programs to comport with a new numbering system alone is prohibitive for any company with a large number of cyber assets. There is no support in the administrative record for the notion that the current numbering system is a problem, or that the proposed combined "all-in-one" standard would improve grid reliability, security, or companies' efforts to comply with the standards. The change to a single CIP-011-1 Standard is arbitrary and of no salient value to anyone. Summarily, Entergy proposes that the: i) Organization and naming/labeling of Version 4 of the CIP Standards remain intact, i.e., simply the fourth iteration of Version 1. ii) SDT should lay FERC Order 706 side by side with CIP-003-3 through CIP-009-3 and make changes specifically attendant to 706 FERC directives - no more, no less. iii) Topical subjects addressed in CIP-003-3 through CIP-009-3 Standards respectively should remain the same, i.e., subject matter organization should not be moved under from under one Standard to another;iv) Concepts already well established and understood throughout the industry created under CIP V1, e.g., CA, CCA, ESP, PSP, etc., should be preserved intact; and,v) Orientation in Version 4 toward protection of "data in motion" is applauded.
9.5	CenterPoint Energy	Break CIP-011-1 up into	As stated above, many entities are now in the compliance phase of the current CIP Standards and have spent a great deal of effort in developing documentation and evidence gathering processes base on the CIP-002 through CIP-009 Standards.

#	Organization	Yes or No	Question 9 Comment
		multiple standards	CenterPoint Energy is concerned about the upheaval required to alter processes and procedures, currently tied to multiple Standards, to match a single Standard. CenterPoint Energy recommends keeping the current format.
9.6	Northeast Power Coordinating Council	Break CIP-011-1 up into multiple standards	Because of the number of requirements involved, combining all into one document will make it more difficult for stakeholders to use, and make it more difficult to assess compliance.
9.7	FirstEnergy Corporation	Break CIP-011-1 up into multiple standards	Break CIP-011-1 up into multiple standards. Multiple standards allows for easier ownership assignment and referencing (indexing) within policies and programs. The new format still provides multiple reference for the same item in multiple locations (e.g. Access), therefore this supports keeping multiple standards.
9.8	City Utilities of Springfield, Missouri	Break CIP-011-1 up into multiple standards	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
9.9	Reliability & Compliance Group	Break CIP-011-1 up into multiple standards	Combining some of the standards may make sense but combining them all does not make it easier to comply, it instead creates an administrative mess by requiring everyone to change all their document references to conform to the new standards and requirements.Some standard combinations that do make sense are physical, electronic and information access (CIP-003 R4, CIP-005 R2-R3, and CIP-006 R2-R6). Also, combining incident response and recovery makes sense.Has a decision yet been made how this would be audited as a single standard? Would we now have compliance violations reported on a requirement level instead of a standard level?

#	Organization	Yes or No	Question 9 Comment
9.10	San Diego Gas and Electric Co.	Break CIP-011-1 up into multiple standards	Due to our previous CIP compliance efforts and all the documentation and Standard Operating Procedures currently in place, SDG&E recommends keeping (as much as possible) the existing CIP Standards and Requirements in place, and augmenting each of the existing Standards with new and modified Requirements. This strategy will allow participating entities to transition to the new version 4 requirements in an easier fashion, while making better use of existing documentation and procedures. We've put a lot of time into the organization, layout, and design of our process and materials and it appears to be a daunting task to revamp all of this to comport with almost completely new Standards. For example, most participating entities would now recognize CIP-004 as having to do with Personnel and Training, whereas combining all the CIP-003 through 009 requirements in CIP-011 just makes it that much more difficult to leverage existing compliance efforts and documentation without a major revamping effort.SDG&E recommends maintaining the current format of standards as CIP-002 to CIP-009, and enhancing the required individual standards as necessary. The existing standards are clear by function and controls - based on general cyber security and systems security practices and controls with the goal of protecting Confidentiality, Integrity and Availability. The implemented standards cover policy, access, change control, monitoring, DR, etc..., and are simple to review, document, communicate, audit and coordinate activities against. Transitioning to a comprehensive single document requires Entities to perform additional translation, communication, implementation and review across departments, organizational structures and systems owners, and increases the potential for communication and task errors, and the potential probability of introducing an operational or security concern.
9.11	E.ON U.S.	Break CIP-011-1 up into multiple standards	E.ON U.S. prefers that individual standards be used instead of the combined standards as outline in CIP-011.

#	Organization	Yes or No	Question 9 Comment
9.12	Matrikon Inc.	Break CIP-011-1 up into multiple standards	For Responsible Entities, their Compliance Teams, their Employees, and their Contractors have all been indoctrinated with the terminology, standards and requirement numbering of CIP 002-009. One reason for continuing a similar number standard is to reduce the confusion for all those involved with compliance, and migration from CIP-002/009 to CIP-010/011.The second reasoning for maintaining similar numbering is the mapping exercise of CIP 002-009 to CIP-010 and CIP-011. If the first priority is to perform the mapping between the two evolutions of the standard, then organically CIP-010/011 will be organized. This will help all affected parties identify the differences, perform gap analysis, and implications to their environment much easier. Unfortunately, all organization will have the exercise of re-authoring a lot of their own NERC CIP compliance procedures to catch up with the new terminology, numbering, and requirements. This will help to maintain compliance with CIP-002/009 while implementing CIP-010/011. Regardless if this is performed by the SDT, every Responsible Entity and Auditor is going to have to do this exercise anyways, with subtle differences.My suggestion is to consider skipping CIP-010, and name it CIP-012. Then take the content related to CIP-003, and organize it into CIP-013. Effectively, putting the next evolution of the standards into the next “decade”, whereby the second-digit is incremented.
9.13	Exelon Corporation	Break CIP-011-1 up into multiple standards	Given the extensive work that has been done to establish monitoring and compliance tracking systems, the wholesale change in format will cause extensive rework to compliance programs (systems, procedures, governance models, etc...). One must ask how this re-work is intended to improve reliability. Unless there is a strong basis for making such a dramatic change to a set of standards that have not been in force for many years, Exelon sees neither need nor value in making such a dramatic change. This change will result in essentially starting from the beginning from a compliance program perspective. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.

#	Organization	Yes or No	Question 9 Comment
9.14	USACE HQ	Break CIP-011-1 up into multiple standards	I suggest to break up the standard into three (3) standards, one (1) for low impact BES Cyber System, one (1) for medium impact BES Cyber System, and one (1) for high impact BES Cyber System. This way it is more clear what is required for each impact level system.
9.15	Progress Energy (non-Nuclear)	Break CIP-011-1 up into multiple standards	If NERC separates into multiple standards, need to make sure the CIP standards are stand alone.
9.16	Indeck Energy Services, Inc	Break CIP-011-1 up into multiple standards	In addition to breaking up the standards by grouping, they should be broken up by facility type and/or function. Not all of these standards apply equally to all facility types or functions. Unmanned facilities with direct communications with a BES control facility need a different set of requirements from a continuously staffed facility without direct communications with a BES control facility. Requirements for a BA are different than for a GOP.
9.17	MWDSC	Break CIP-011-1 up into multiple standards	It is confusing that the tables for each major category only show those requirements with different impacts, while there are other requirements that apply to all impacts. Suggest adding a matrix of all the requirements by a major category showing all the requirements and impacts, not just the ones which differ. Having one standard would require the entire standard to be re-issued for any change. This may cause more confusion whether anything else changed and create more wasted paper. Suggest multiple standards or using a numbering scheme such as CIP-011-1.1, CIP-011-1.2, CIP-011-1.3, etc to separate the requirements by major categories. If there is a change to a major category, the numbering would be CIP-011-1.2a, CIP-011-1.3c, etc.
9.18	Platte River Power	Break CIP-	It would be clearer if the requirements were organized based on their objectives:

#	Organization	Yes or No	Question 9 Comment
	Authority	011-1 up into multiple standards	physical security, system security, boundary security, personnel management, access, etc. One document would be fine if the requirements matched up with the standards and the sub-requirements matched up with the requirements.
9.19	Allegheny Energy Supply	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements
9.20	Allegheny Power	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.
9.21	EEI	Break CIP-011-1 up into multiple standards	It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.
9.22	MidAmerican Energy	Break CIP-011-1 up	MidAmercian Energy does not prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements. The revolutionary approach proposed

#	Organization	Yes or No	Question 9 Comment
	Company	into multiple standards	will cause confusion, which may adversely affect the reliability of the BES. The version 4 standards should be built upon the existing standards to avoid the unnecessary confusion that will be introduced during the implementation of CIP-011. Rewrite CIP-011 and apply the requirements to existing CIP-003 thru CIP-009 standards.
9.23	CWLP Electric Transmission, Distribution and Operations Department	Break CIP-011-1 up into multiple standards	Monitoring changes to the requirements would be easier if they were separated into different standards.
9.24	Con Edison of New York	Break CIP-011-1 up into multiple standards	Most owners of BES equipment have multiple departments that manage different corporate functions. These departments include Information Resources, System Operations, Human Resources, Relay Protection, Engineering, etc. Organizing the CIP requirements into topic-specific standards (as was done for CIP-002 through CIP-009), will facilitate corporate management of compliance.
9.25	Michigan Public Power Agency	Break CIP-011-1 up into multiple standards	Multiple standards that are logically separated is preferred. However, if separated the standards still should be approved as a complete set.
9.26	PacifiCorp	Break CIP-011-1 up into multiple standards	PacifiCorp does not prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements. The revolutionary approach proposed will cause confusion, which may adversely affect the reliability of the BES. The version 4 standards should be built upon the existing standards to avoid the unnecessary confusion that will be introduced during the implementation of CIP-011. Rewrite CIP-011 and apply the requirements to existing CIP-003 thru CIP-009 standards.
9.27	Florida Municipal Power	Break CIP-	The addition of sub-headings into CIP-011 is illustrative of the need to separate them.

#	Organization	Yes or No	Question 9 Comment
	Agency	011-1 up into multiple standards	From a presentation perspective, e.g., most frequency violated standards, we would be faced with tough decision of either having one standard with a very large bar in a top 10 bar chart, or possibly having multiple CIP standards is the bar chart, until the Industry gets used to the new standards. Either way is politically difficult, so, the simpler approach is probably the preferable approach of multiple standards on different security topics.
9.28	APPA Task Force	Break CIP-011-1 up into multiple standards	The APPA Task Force believes the addition of sub-headings to CIP-011 is illustrative of the need to separate this standard into multiple standards. We also feel with multiple standards the revision process would be simplified. If only one section needs to be revised, then NERC could just post that particular section for industry comment.
9.29	Emerson Process Management	Break CIP-011-1 up into multiple standards	The original setup seems indicating some logic on how cyber security should be addressed. Also, it has been there for several years. Most people probably have become used to the titles and subjects.
9.30	Southern California Edison Company	Break CIP-011-1 up into multiple standards	The section of standards that deal with controls should be divided into components that are grouped thematically. For instance, management of personnel may contain all requirements pertaining to training, background checks, etc., as one standard. Another standard should be used for governance functions such as policy making and management, audit documents, change management, etc. A third standard for Access Management can be used to list in detail end-to-end access controls for interactive access that is electronic, escorted and unescorted physical access and access to information. Boundary protections, physical and electronic, can be addressed as a family of security controls along with system security requirements as a fourth standard. A section that describes priority of controls within each requirement, in addition to a VRF/VSL document, should be provided so that RE's can implement controls at a granular level even within the High-Medium-Low framework.SCE supports the

#	Organization	Yes or No	Question 9 Comment
			modification of the CIP standards from a family of eight controls in the current version, and the reduction of the number of sub-levels within requirements. But on the other hand, combining all controls into "one standard" is a cause for concern.
9.31	LCEC	Break CIP-011-1 up into multiple standards	The standard grouping in CIP11 will result in a negative perception as to the progress industry is making in improving cyber security of the BES. Consider individual standards or a new approach to metrics reporting that focuses on the security domain versus the standard.
9.32	Old Dominion Electric Cooperative	Break CIP-011-1 up into multiple standards	This draft is far too cumbersome. Breaking up the requirements will allow emphasis to be placed on categories that may be more critical to security. Breaking up the requirements will also allow for much easier application.
9.33	Pepco Holdings, Inc. - Affiliates	Break CIP-011-1 up into multiple standards	We agree with EEI's comments.
9.34	We Energies	Break CIP-011-1 up into multiple standards	We Energies agrees with EEI comments: It would be easier for entities to recognize and understand the similar or different requirements in version 4 if they were broken up in a manner similar to legacy CIP-003-009. Many organizations have made significant investments in training, policies, procedures, and document management systems that are based on the legacy CIP standard Requirement numbering structure. Staying with the legacy structure, to the degree that it is possible, may reduce stranded investment that needs to be recreated simply as a function of the name and numbering of the requirements.

#	Organization	Yes or No	Question 9 Comment
9.35	Luminant	Keep CIP-011-1 as one document	future changes that do not impact the compliance domentation numbering should be considered
9.36	FEUS	Keep CIP-011-1 as one document	Having CIP-011-1 as one document makes it more streamlined and is easier to follow. The concern FEUS has is how multiple violations of several different sub-requirements will be looked at by the compliance enforcement agencies. If an entity is found in violation of CIP-011-1 R4 for example and is later found in violation of CIP-011-1 R26 will this be considered a second violation? If so, FEUS would prefer CIP-011-1 to be grouped into separate standards.
9.37	Public Service Enterprise Group companies	Keep CIP-011-1 as one document	Having the requirements in a single standard significantly improves understanding and ease of reading.
9.38	Ameren	Keep CIP-011-1 as one document	It is much easier to find all the requirements when all contained is a single document and the chance of discrepancies between documents is greatly reduced. However, the CMEP should be updated to monitor and report violations by standard and requirement not just standard. Otherwise, CIP-011 will always be in the list of Top 10 most violated standards and create a misleading impression that utilities cannot figure out how protect the reliability of the BES.
9.39	Southwestern Power Administration	Keep CIP-011-1 as one document	Keeping the controls in one document as proposed is preferable; provided that the intent is not that ALL requirements in CIP-011-1 have to be audited as a family of requirements.
9.40	Dairyland Power	Keep CIP-011-1 as	One document is better.

#	Organization	Yes or No	Question 9 Comment
	Cooperative	one document	
9.41	Green Country Energy	Keep CIP-011-1 as one document	One document makes it a lot cleaner for a smaller entity to deal with.
9.42	Progress Energy - Nuclear Generation	Keep CIP-011-1 as one document	Security controls included in CIP-011-1 are similar to the Security Controls established by Nuclear Energy Institute (NEI) 08-09, Revision 6, Appendices D and E. These security controls are based on one or more National Institute of Standards and Technology (NIST) 800 series standards and have been accepted by the Nuclear Regulatory Commission (NRC) in a letter dated May 5, 2010. Alignment of CIP security controls with security controls based on NIST 800 series standards and implemented in NEI 08-09, Revision 6, for nuclear plant systems would prevent regulatory uncertainty and potential dual regulation of a single system.
9.43	Consultant	Keep CIP-011-1 as one document	Subject to the following:1. Requirement number should be consistent with the Requirement table numbering. For example, currently requirement 3.1 Cyber Security Training does not relate to Table item 3.1 Electronic Access. The result is two items that would be referenced as CIP-011 3.1 on completely different topics.2. Every requirement should have a related table. Currently R1 & R2 do not have related tables for applicability. It is 'bad practice' to assume the interpretation that those requirements without a table apply to everything.3. The 'local definitions' should be gathered in a separate definitions section and numbered. Lacking a definitions section there is no convenient mechanism to refer to local definitions.4. While I understand the expressed opinion makes the standard easier to use, I don't agree with that opinion. The defined terms related to this standard should be listed in a separate section. My opinion is that the current format of the local definitions is more confusing than clarifying.5. Based on the CIP Standards Workshop information, I would suggest the Requirement statment (R1, R2, R3, etc.) be a statement of the requirement objective, and the Table rows be

#	Organization	Yes or No	Question 9 Comment
			implementing requirements for that objective. This approach should also resolve items 1 & 2 above.
9.44	RRI Energy	Keep CIP-011-1 as one document	The previous CIP-003 through CIP-009 required cross-referencing between the standards and standard owners to get it right. CIP-011 is much easier to follow and understand.
9.45	Bonneville Power Administration	Keep CIP-011-1 as one document	The single document format clearly states the requirements unlike the current standards which link to one another but do not clearly link the requirements.Having CIP-011-1 as one document rather than multiple standards is great. All of the requirements are in one place and easy to find.
9.46	Detroit Edison	Keep CIP-011-1 as one document	The tables holding the sub-requirements are a good feature that enhances readability. CIP-011 R3 and R4 have some requirements outside of the table and some in the table. Please move all sub-requirements to table format so each requirement would become a paragraph followed by a table with subrequirements. This will help minimize confusion caused by having a requirement and a table entry with the same number.
9.47	Dominion Resources Services, Inc.	Keep CIP-011-1 as one document	Using a single standard for all requirements is preferred, however the format internal to the single standard appears to be inconsistent. For example, some requirements are in paragraph form while others are embedded in a requirements Table. All requirements should be contained within a requirements Table. Where possible, information preceding the table should be used only to state the context and establish the security objective or intent behind the requirements.
9.48	Manitoba Hydro	Keep CIP-011-1 as one document	We agree with the proposed approach which creates a clear list of security requirements within a single standard. This addresses some of the complexity with the existing cyber security standards. We are, however, concerned about the current compliance monitoring and enforcement structure where the magnitude of fines and sanctions are levied based on prior violations, and the violations are reported per standard. The

#	Organization	Yes or No	Question 9 Comment
			proposed standard contains over one hundred requirements and sub-requirements, which increases an entity's exposure to multiple violations for a single standard, and increases the exposure of the industry to a large number of violations to a single standard.
9.49	Hydro One	Keep CIP-011-1 as one document	We agree with the proposed format for simplicity purposes. However, by consolidating the current version 3 standards into one document, this new CIP-011 standard would become one of the NERC's standards with the largest number of requirements. This could potentially make it "the most violated" one as well consequently impact the amount of monetary sanctions. If the proposed format is adopted, special compliance consideration should be adopted when dealing with violations
9.50	Minnesota Power	Keep CIP-011-1 as one document	With the requirements in a single document, it seems that it will be easier to arrange and consolidate requirements to alleviate the duplications and contradictions which have plagued the preceding CIP standards.
9.51	Tenaska	No preference	A personnel training issue can cause a violation of the whole standard that will be looked at as the same as a Cyber System boundary problem (Outsider Scanning). Until violations reporting and sanctions are reported at the requirement level only, then this could have a disproportionate impact on the entity relates to potential impact on the BES.
9.52	Network & Security Technologies Inc	No preference	Believe the SDT's time and effort are better spent on defining well-understood and auditable requirements that will enhance BES security & reliability than on trying to force-fit new/updated requirements into existing document structures.
9.53	US Army Corps of Engineers, Omaha Distirc	No preference	Combined this standard covers a very large number of requirements. Note the drafting committee divided the standard into several logical groupings for the presentation of the standard.

#	Organization	Yes or No	Question 9 Comment
9.54	ERCOT ISO	No preference	Either option is acceptable. Having them in one document could prevent public documentation of specific areas of weakness for an organization as audit results are public information and published on the NERC website. It also eliminates the need for circular referencing that is in the current CIP-002 to CIP-009 (e.g., CIP-005 R1.5).
9.55	Southwest Power Pool Regional Entity	No preference	Having all of the requirements in one document as opposed to many makes no difference to the compliance monitoring and enforcement process as long as Violation Severity Levels and Violation Risk Factors do not roll up higher than the main-level enumerated requirements. The advantage of keeping everything in one document is simpler version management and reducing the need for cross-standard references. The disadvantage is that more of the requirements will potentially be exposed to comments whenever the standard is being updated. Additionally, multiple standards permit parallel modification efforts whereas a single standard may result in single-threaded modifications over a prolonged development and approval timeframe.
9.56	Pacific Gas & Electric Company	No preference	Keeping CIP-011 as one document reduces complexity and makes overall understanding easierBreaking CIP-011 into multiple documents facilitates certain compliance and accountability aspects
9.57	SCE&G	No preference	The SDT should consider the advantages of breaking the Standard into multiple standards, as far as implementation goes. Some requirements will require more time to implement than others. Having the standard broken apart may make distinguishing these timeframes easier.
9.58	Southern Company	No preference	The tabular format for the requirements section is an excellent vehicle to capture the individual requirements. This should be expanded to include all requirement items. The numbering in the tables should be made unique to match the associated requirements in the standards body. (i.e., R3.1 is related to security training while table entry 3.1 is related to electronic access.)Sections of the table which do not apply should be marked N/A.

#	Organization	Yes or No	Question 9 Comment
9.59	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	No preference	Violations are by requirement, so whether it is one standard or multiple standards makes no difference.
9.60	Independent Electricity System Operator	No preference	We understand the need for this standard to take care of cyber security concern when there does not currently exist an across-the-board cyber protection standard that applies generically to all sectors that utilize cyber components and cyber access for control and data exchange. However, over time, we urge NERC and the electric industry to assess if indeed it needs to have its own cyber protection standards at all. Cyber protection is not unique to the electric industry. Other sectors - airline industry, national security/ defense, financial sector, banking system, etc. all employ a high level of cyber security to protect fraud and invasions. Wouldn't the electric industry be better served if owners of BES Cyber Systems be required to adopt similar practices of these other sectors as opposed to developing it own very detailed set of requirements which, for the most part, seem to replicate the other sectors' requirements?It will be desirable to have a generic set of Cyber protection standards that is applicable to all sectors that use Cyber Systems - may they be for BES control or access to airline reservation, air traffic control, e-banking, security trading, etc. NERC and the electric industry should take the lead to initiate a continent-wide effort to consolidate all such standards and practices to avoid redundant efforts.These comments notwithstanding we still offer some comments on the remaining questions.
9.61	Verizon Business	Keep CIP-011-1 as one document	One document eliminates potential confusion about the use of the correct version. However, during the initial implementation phase, there may be multiple revisions for CIP-011 being issued each month/quarter.

10. The Purpose of draft CIP-011-1 states, "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES." Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Suggestions for the purpose statement for the draft CIP-011 standard included several suggestions for rewording as well as comments expressing confusion around the term BES Cyber Systems. Several commenters expressed that the owner of BES Cyber Systems should have responsibility for compliance with the Standards and the Purpose statement did not reflect this.

In response to the industry comments received for draft CIP-011, the CSO706 SDT decided to divide up the draft CIP-011 requirements and include them in the multiple Version 5 CIP Standards (CIP-003 through CIP-011). Therefore, the purpose statement included with the draft CIP-011 no longer applies.

#	Organization	Yes or No	Question 10 Comment
10.1	PacifiCorp	Agree	: PacifiCorp agrees with EEI's suggested revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."
10.2	WECC	Agree	Agree with the genearal purpose however, The term "necessary cyber security protection" in the purpose statement has no meaning without a frame of reference. The purpose statement may be used to clarify intent where the standard language is ambiguous or vague, so it should explicitly state the objectives of the standard.The phrase "...that perform functions essential to reliable operations of the interconnected BES" in the purpose statement is redundant. BES Cyber Systems are defined elsewhere so this clause adds confusion at best, and contradicts at worse.
10.3	Southwest Power Pool Regional Entity	Agree	As an overall purpose, the statement is OK. Consider addressing the issue of "responsibility" as it pertains to multiple entity aspects, including joint ownership

#	Organization	Yes or No	Question 10 Comment
			agreements, different owners versus operators, and the like.
10.4	Old Dominion Electric Cooperative	Agree	I agree under the assumption that this is in line with the enabling legislation in the Energy Policy Act. I disagree that this is the best way to go about achieving this goal.
10.5	Green Country Energy	Agree	I agree with the concept, however as I will repeat through the remainder of the comments, A guidance document is needed to address key points desired to be accomplished by these policies. This will also reduce the subjectivity during audits of this and all the following requirements
10.6	Progress Energy (non-Nuclear)	Agree	It is still unclear if cyber security implies that an external communications capability is available. Definitions and references seem to indicate that we can have a BES cyber system component without external connectivity.
10.7	US Bureau of Reclamation	Agree	Recommend that the Drafting Team change "Functional" to "Registered" in the 1st line of the Purpose. Add "they" between "that" and "execute" in the 3rd line of the Purpose statement.
10.8	Minnesota Power	Agree	This purpose statement is generally acceptable, with clarification or correction to the following: o What is the definition of “responsible”? Minnesota Power recommends changing this to “own” as is stated in CIP-010-1, R1. o The reference to “Functional Entities” should be replaced with “Registered Entities.” “Functional Entities” is not a defined term.
10.9	San Diego Gas and Electric Co.	Agree	While SDG&E agrees with the purpose of CIP-011 as applied to the various requirements, we would like to see additional language that would help clarify the meaning of the phrase “responsible for”. What if an entity owns a particular asset but does not operate it?
10.10	ISO New England Inc	Disagree	- Please provide additional clarification. Especially with regard to “necessary cyber security protection”.- Suggest changes from “cyber security protection” to “cyber

#	Organization	Yes or No	Question 10 Comment
			security controls".
10.11	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Advise replacing "are responsible" with "operate." Where one Entity may own the BES Cyber System, and another Entity operates the same BES Cyber System, it must be clear who will be responsible for developing and implementing the policies. In many instances, the owner of a BES Cyber System only has monitoring capability, and no control or supervisory role in the BES Cyber System. Owners should not be responsible for creating policies for Systems they do not fully understand; owners should only be responsible for securing the BES Cyber System Components that they operate.
10.12	FirstEnergy Corporation	Disagree	As stated in our opening remarks, we fundamentally oppose the change in terminology. Additionally we disagree with the need for functional categorization as described in Attachment I. Therefore, we do not support the purpose statement of CIP-011.It is suggested that the proposed definitions for BES Cyber System and BES Cyber System Component could be combined to redefine the existing Critical Cyber Asset term allowing industry to better leverage its existing CIP implementation.Additionally, there is a concern, in going with the concept of "BES Cyber Systems" that it will expand beyond the systems that are directly responsible for the reliable/safety of the BES and into business systems.
10.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
10.14	ERCOT ISO	Disagree	Consider: "To ensure Responsible Entities develop cyber security programs to provide for appropriate protection of the BES Cyber Systems for which they are responsible that execute or enable functions essential to reliable operation of the interconnected BES."
10.15	Consultant	Disagree	Cyber security policies or cyber security protection do not 'execute' functions essential to reliable operation of the BES. Suggest removing the word 'execute'."interconnected BES" is not a defined term. Suggest removing the word 'interconnected'.

#	Organization	Yes or No	Question 10 Comment
10.16	US Army Corps of Engineers, Omaha Distirc	Disagree	Delete everything after "for which they are responsible." It reads awkward and is merely restating the meaning of BES Cyber System.
10.17	Kansas City Power & Light	Disagree	Do not agree with ensuring security policies in the purpose. The express purpose of these requirements should be to identify the cyber systems that require protection and the level of protection to achieve. There is no need to include a purpose of entering into the management of an organization and the levels an organization deems necessary to achieve compliance with the these CIP Standards or any other NERC Reliability Standard.
10.18	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing the statement as follows: "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems."
10.19	American Municipal Power	Disagree	I feel the purpose is not based on reliability. The purpose should not restate the applicability section.
10.20	Wolverine Power	Disagree	I have a concern with how to detrmine hat constitutes a "BES Cyber Ssystem" I don't think the standards are clear.See comments listed for 1.a fro explanation and proposed solution
10.21	Turlock Irrigation District	Disagree	Is the use of the words "the BES Cyber Systems for which they are responsible" above meant to be the same as the words "the BES Cyber Systems that it owns" which are used in CIP-010-1 R1? The Purpose of CIP-011-1 focuses compliance responsibility on the entity that is responsible for the BES Cyber Systems while CIP-010-1 R1 focuses compliance responsibility on the owner of the BES Cyber Systems.
10.22	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."

#	Organization	Yes or No	Question 10 Comment
10.23	NextEra Energy Corporate Compliance	Disagree	NextEra believes implementation responsibility of protection methods should tie back to facilities under the entities control and ownership.
10.24	Reliability & Compliance Group	Disagree	Recommend adding the words “and implement”. Also the phrase “execute or enable functions essential to reliable operation...” needs a more concise definition.
10.25	Independent Electricity System Operator	Disagree	See response to Q9.
10.26	Network & Security Technologies Inc	Disagree	Suggest replacing “enable functions essential to...” with “support functions essential to...”
10.27	Allegheny Energy Supply	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.28	Allegheny Power	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.29	EEI	Disagree	Suggested Revision:”To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES.”
10.30	Nuclear Energy Institute	Disagree	The phrase “and that execute or enable functions essential to reliable operation of the interconnected BES” should be struck as it is redundant to the definition of BES Cyber Systems.
10.31	APPA Task Force	Disagree	The purpose is not to “develop ... policies” as the first item in the list currently indicates. The purpose is to protect cyber systems from attack, with policies, procedures, etc., to support that purpose. The APPA Taskforce suggests inserting the following “Purpose”

#	Organization	Yes or No	Question 10 Comment
			section:Purpose: To safeguard the reliability of the Bulk Electric System (BES) by protecting BES Cyber Systems from attack through the use of appropriate policies, procedures, tools and other resources.The APPA Task Force further recommends that each of the Requirements be reworded to separate out the stated objective to be accomplished from the text of the actual requirement and to state the objective prior the text of the Requirement. Auditors should not be placed in the position of having to evaluate if an entity has met the objective stated in the requirement, since this is essentially a subjective judgment. We feel this objective should not be part of the requirements. Here is one example of our proposed format illustrated with Requirement R5: Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R5 - Physical Security for BES Cyber Systems. The APPA Task Force recommends adding the following "Objectives" section after the Purpose in this standard:A. Introduction 1. Title: Cyber Security - BES Cyber System Protection 2. Number: CIP-011-1 3. Purpose: To ensure Responsible Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES. 4. Objectives:a. Personnel Training, Awareness, and Risk Assessment: To ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems. b. Physical Security for BES Cyber Systems: To prevent and/or detect unauthorized physical access to BES Cyber Systems.c. Personnel Risk Assessment: To ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. d. etc...If the Objectives are not incorporated into the Introduction, we recommend they be removed from the requirement all together. If the team determines they are necessary, they must be in a separate sentence prior to the requirement. See comments on Question #12 and all other questions regarding the requirement title.
10.32	Florida Municipal Power Agency	Disagree	The purpose is not to "develop ... policies" as the first item in the list currently indicates. The purpose is to protect cyber systems from attack, with policies, procedures, etc., to support that purpose. FMPA suggests the following:np"To safeguard the reliability of the

#	Organization	Yes or No	Question 10 Comment
			Bulk Electric System (BES) by protecting BES Cyber Systems from attack through the use of appropriate policies, procedures, tools and other resources."
10.33	Indeck Energy Services, Inc	Disagree	The purpose of CIP-011, assumes that every facility registered with NERC is a cyber threat. It needs to differentiate functional entities to determine the impact on BES ALR. The functions identifies in Attachment I of draft CIP-010 are all important. Many of them are provided by hundreds or thousands of facilities. The cyber policies envisioned cannot ensure (that is guarantee) that there will be no blackouts due to cyber attack. [suggestion] "To require Functional Entities to develop, coordinate and apply adequate cyber security protection to the BES Cyber Systems for which they are responsible and that will achieve BES Adequate Level of Reliability." The coordination is to avoid unnecessary duplication of cyber security protection. This may require a different type of requirement that links connected parties, such as TO and GO, as to protecting particular facilities.
10.34	Manitoba Hydro	Disagree	The purpose statement appears to be missing words in the last line. Consider adding the words 'as outlined in this CIP-011-1' after the word 'responsible'.
10.35	Constellation Energy Control and Dispatch, LLC	Disagree	The purpose statement will need to be developed for each standard if CIP-011 is broken up into its major components.
10.36	Platte River Power Authority	Disagree	This comment is referring to an earlier comment suggesting a mechanism for identifying a "Responsible Entity" who is responsible for implementing and demonstrating compliance. With the "Responsible Entity mechanism in place I would suggest the following revision:To ensure the Responsible Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems that execute or enable functions essential to the reliable operation of the BES.
10.37	Entergy	Disagree	This Requirement uses the qualifier: "for which they are responsible." In Requirement 1 of CIP-010-1 (Question 3) the qualifier is "that it owns" - these two requirement statements must be consistent one way or the other.

#	Organization	Yes or No	Question 10 Comment
10.38	ReymannGroup, Inc.	Disagree	Vendor management and due diligence of 3rd party vendors is a growing area of risk across multiple industries, including the bulk power system. We believe the "Purpose" language should be enhanced to clearly cover the Functional Entities' internal practices and those of its 3rd party resources. This should include all 3rd party vendors that may have on-site or off-site access to the BES hardware, software, or data. For example, the information security risk associated with a growing use of data recovery service providers is not addressed in the NERC guidelines. Data Recovery is defined in Wikipedia as the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. The definition of a BES includes programmable electronic devices such as hardware, software, and data. It makes sense that as the demand for such electronic storage devices continues to rise, more equipment will be damaged or will fail due to daily wear and tear, physical damage, data corruption, or natural disasters (e.g., flood, fire, etc.) If backup copies of lost data on the BES are not available, the need for data recovery services will increase to keep pace with the use of BES technology. It could be made more clear to emphasis that Cyber security protections are applicable while the BES is in operation and off-line. BES could be taken off-line for repair or other incidents such as a damaged hard drive and recovery of BES data, which will require a 3rd party vendor to recover sensitive data from the BES device.We recommend that NERC consider adding a new Requirement for Vendor Management as described in our comments to Security Governance and Policy (R1) and updating the R25 and R30 guidelines to address this 3rd party vendor data recovery risk. It is a very small aspect of day-to-day operations in the scheme of the Entity's priorities, which is why it has gone unnoticed - until now. As one regulator commented to us recently, "this is not a potential problem - it is a real problem." It can create a huge risk with a huge downside, if it is not controlled. Most organizations don't even realize that this "sleeper risk" exists, until it is too late. The good news is that with minor updates to proposed guidelines, NERC can educate entities and others about the risk associated with the use of data recovery service providers and provide meaningful tactical guidance on how to manage such risk. The current initiative to revise the CIP Cyber Security Reliability Standards is a timely opportunity to take the initial steps.

#	Organization	Yes or No	Question 10 Comment
			Perhaps some organizations have included data recovery security practices and protocols in incident response or recovery planning. The challenge here is that it usually requires a material event to activate the incident response or recovery plans. In such instances, these plans do not address the proper day-to-day use of data recovery service providers that would not be considered a material event. Frequently, the use of a data recovery service provider does not trigger a formal recovery plan or incident response plan. It is unlikely that most entities would execute a recovery or incident response plan to recover data from a failed BES device in the normal course of day-to-day activities. In the interim, it would be helpful to Functional Entities and others if NERC issued supplemental guidance specific to this topic. This will help establish an immediate awareness of the risk and share much needed guidance on appropriate due diligence and security protocols for data recovery service provider activities, selection, and use. Specifically, the data recovery risk exists from a lack of information security protocols and practices in the vetting, selecting, and use of data recovery service providers.Whether a breach of sensitive information occurs from a hacker, cyber threat, insider threat, or a data recovery service provider, the potential cost, fines, reputational damage, and loss of trust that an organization would experience is huge. In short, data recovery service provider risk can create as much damage as other risks that are addressed in existing NERC guidelines, if adequate controls are not defined and implemented. A typical security and compliance budget will allocate funds to protect people, information, and assets within the perimeter. Many entities are also focused on protecting data on the inside of their organization from outside attacks. Data recovery, however, frequently falls into a low priority category that does not pop-up on the CISO's radar or in an information security risk assessment. The need for data recovery is frequently associated with an immediate sense of urgency, e.g., the data contained on the damaged storage device must be recovered right away. o Help Desk personnel or office technicians are usually tasked with the responsibility of selecting an outside third party vendor to recover the data quickly. o Such third party vendors may or may not be listed on an approved vendor list. o Frequently, the due diligence and selection process of such a vendor is limited to its financial stability, the cost of its services, and a fast

#	Organization	Yes or No	Question 10 Comment
			“turnaround time.”According to an independent national study - Security of Data Recovery Operations - published by the Ponemon Institute in December 2009 and conducted among IT security and IT support practitioners, there is a gap in security guidelines when selecting data recovery service providers. Specifically, o Sixty-four percent of the respondents decentralize the selection for data recovery vendors to the local level, e.g., Help Desk, while 24 percent are not sure how the vendor is selected. o Sixty-nine percent of the respondents do not have or are unsure if they have a policy for ensuring the protection of data during the recovery process. o Forty-nine percent say IT security is not involved in the selection process. o Only 20 percent believe data security is a major selection criterion. o Eighty-two percent say that it should be.A large percentage of respondents in this study (83 percent) reported at least one data breach in the past two years. Of the 83 percent who said the organization had a data breach, 19 percent said the breach occurred when a drive was in the possession of a third-party data recovery service provider. Forty-three percent of those respondents who said the breach occurred while at the vendor say it was due to a lack of data security protocols. Most organizations also have some additional backup and recovery procedures that overshadow the sense of urgency for more attention to data recovery practices on devices that were not backed up. In short, even with a strong backup recovery program, data recovery needs still arise. Seventy-nine percent of the respondents to the Ponemon study noted that their organizations have used or will continue to use a third-party data recovery service provider to recover lost data.Additional guidance is needed on how to extend current information system program practices to clearly address the protection of sensitive data, while it is in the possession of a third party service provider for data recovery. If the Entity has a strong vendor risk management program, it should include ALL vendors that have access to sensitive data, including data recovery vendors. Mandated vendor management practices apply to all stages of the information life cycle. Specific to data recovery vendors, this includes:âˆš Pre-selection and negotiation of Master Service Agreements with appropriate vendors. These should be reviewed by a risk management committee and audited on an annual basis.âˆš Due diligence of all third party vendors (e.g., financial stability, client references, information security

#	Organization	Yes or No	Question 10 Comment
			practices, etc.)âˆš Verification of the vendor's security procedures to govern the transfer of devices and sensitive information.âˆš Proof of internal information technology controls and data security safeguards, e.g., ISO 27001 certification, NIST SP 800-53 Audit Report, FFIEC Service Provider Examination Report, BITS Shared Assessment Report, or SAS 70 Type II Audit Report (especially if the data recovery involves financial information). The appropriate certification and audit report will vary depending on the service provider's client base.âˆš Proof of current training and certifications of engineers in all leading encryption software products and platforms.âˆš Adequate chain-of-custody documentation and network security.âˆš Vetted and performed background checks of its employees.âˆš Adequate procedures for the secure and permanent destruction of devices, when required.âˆš Capabilities for encryption of data files in transit and storage.âˆš Adequate clean room facilities, e.g., certified ISO 5 (Class 100).âˆš A security procedure for the analysis of the information and device upon return to the organization to ensure malware and other malicious software has not been loaded.The lack of information security protocols and practices in the vetting, selecting, and use of data recovery service providers is not a potential problem - it is a real problem! NERC guidelines are a key resource that can help educate functional entities and others to this sleeper risk and identify prudent risk management practices and controls.
10.39	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
10.40	We Energies	Disagree	We Energies agrees with EEI: Suggested Revision:"To ensure Responsible Entities develop cyber security policies and apply cyber security protection to the BES Cyber Systems for which they are responsible and that perform or enable functions essential to reliable operation of the BES."
10.41	GTC & GSOC	Disagree	We recommend the language should be consistent with CIP-010 "owns" versus "responsible for." As indicated in comments on 1.b above, "owns" may be problematic.

#	Organization	Yes or No	Question 10 Comment
10.42	Xcel Energy	Disagree	We suggest the Purpose be revised to state "...and apply necessary cyber and physical security protection..."
10.43	Verizon Business	Agree	Any "carryover exceptions" from CIP-002 to CIP-009 need to be identified. Specifically, OSI Layer 2 Protocols need to be explicitly addressed.

11. Requirement R1 of draft CIP-011-1 states, "Each Responsible Entity shall develop, implement, and annually review formal, documented cyber security policies that address the following for its BES Cyber Systems:" and then provides a list of topics that must be addressed. Do you agree with this proposal and list? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many commenters requested more clarity regarding the terms used (including the following: "formal," "annually," "boundary protection," "security roles and responsibilities," "personnel," etc…). Commenters requested to have the terms used throughout the standard defined in this section. Additional clarity was sought in terms of the policy expectations, purpose, and structure. Specifically, there were numerous questions about what is meant by "policy language," along with concerns about how to demonstrate compliance with a policy. Some commenters also noted that the policy requirements were too prescriptive. There were some comments that led the SDT to believe that there was some possible confusion surrounding general policy hierarchy.

The SDT agrees with the need for additional clarification and clearer expectations with regard to the policy. The drafting team has provided clarification through the addition of guidance material related to items that should be included in policy, and has implemented a style for the measures in each requirement that can be used as an aid in setting clear expectations for possible audit evidence.

Some commenters raised questions about the requirements with respect to the Senior Manager; specifically with concerns about delegation and the potential for conflict with R3, or claims of double jeopardy between R1 and other requirements.

The SDT appreciates the concerns about double-jeopardy issues and the prescriptive nature of the requirements. As such, the SDT has proposed moving the prescriptive elements of the requirement to guidance. This approach will allow the Responsible Entity greater flexibility to create a policy that is meaningful for its unique environment, while still providing the foundation necessary for an effective cyber security program.

#	Organization	Yes or No	Question 11 Comment
11.1	Entergy	Agree	"Annually" must be defined. At least once every twelve months? At least once per calendar year (this could extend past 12 months). Please clarify.
11.2	Green Country Energy	Agree	Agree with the list, however I really see the need for a reference document or footnotes pointing to sources for guidance on the expectations for these policies. Because the policies / requirements were designed not to be to prescriptive they in turn need references to give some expectations as to the points to be addressed within the

#	Organization	Yes or No	Question 11 Comment
			policies. This will allow flexability as to tailor the policy to each business, the policy will meet with the objectives of NERC / FERC and make the policies easier to audit. Is this what results based standards is all about...
11.3	Covanta Energy	Agree	Annually may be needed due to frequent challenges and changes to cyber hacking techniques.
11.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
11.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent, but believes the following improvements should be made:What does “formal” mean, does the drafting team intend a Company Policy?Terms used in later requirements ought to be defined here, such as unauthorized access, Cyber Security Incident(s), and electronic access controls.Terms that are ambiguous, such as “Boundary protection” and “media sanitization” ought to have definition boxes associated with them. In general, definition boxes should be adjacent to the term as it is first used in the standard. Alternatively, a definitions sections such as is used in typical contracts could be a new standard section for those definitions that are used only in this standard that are not included in the Glossary.It should be clear the “Personnel ...” used in 1.4 includes external contractors.1.7 seems to encompass 1.5, 1.6 and 1.8, consider making 1.5, 1.6 and 1.8 sub-bullets of 1.7
11.6	National Grid	Agree	In 1.2 please elaborate on “security roles and responsibilities”. What is the SDT looking the entities to include as part of this document?
11.7	Minnesota Power	Agree	Minnesota Power would like to see more detail regarding each of the topics on the list to help clarify the expected content of these policies. For example, item 1.3 requires the naming of a single senior management official, with no mention of the ability to also name delegates. Yet, Requirement R3 includes the following language: “...that are approved by the single senior management official...or their delegate...”

#	Organization	Yes or No	Question 11 Comment
11.8	Bonneville Power Administration	Agree	NOTE: This following comment deals more with structure of the document than it does with content: NIST SP 800-53 lists 19 families of security controls for Government systems. Although the purposes of 800-53 and CIP-011 are not equivalent, there seem to be 800-53 families missing from CIP-011 that address areas that should be of interest in CIP-011. Even if the individual controls are addressed in CIP-011, listing the families would be useful. In particular, it is unclear why Audit and Accountability, Contingency Planning, Identification and Authentication, Personnel Security, System and Communications Protection, System and Information Integrity, and Program Management are not addressed. We believe that incorporating these would be an improvement to the document. In the CIP versions 1, 2 and 3 standards organizations have had numerous and almost endless discussions about what “annual,” “annually review,” etc. means. Hours have been spent trying to figure out what these terms mean. Some have said that “annual” means within 13 months. Annual meaning “within 13 months” makes absolutely no sense. It would be extremely helpful to the industry if clarity were provided in CIP-011-1. The debate needs to end. There appear to be four different phrases that could be used to provide more clarity:1. “at least once every 12 months” - let’s assume that the organization reviews all of the various policies referenced in R1 on July 15, 2010, and again on March 15, 2011. Using this phrase and example, however, raises a couple of questions. When must the next review be completed? Is it no later than July 15, 2011, or no later than March 15, 2012? In other words, is there a window in which "annual" events must occur, "12 months +/- a month" or if you perform something early for efficiency's sake, does your annual date reset to the earlier date?2. “every 12 months” - the review would occur on the same date each year. This would be virtually impossible to manage. 3. “within 12 months of the last . . .” - in this case let’s assume that a review is performed on March 15, 2010. The next review would have to occur no later than March 15, 2011, but could occur earlier (let’s say it occurred on December 15, 2010). If it occurred on December 15, 2010, the subsequent review would have to occur no later than December 15, 2011.4. "anytime during the calendar year" - which would give the organization maximum flexibility in accomplishing the compliance activities.The Standards Drafting Team (SDT) should

#	Organization	Yes or No	Question 11 Comment
			provide more clarity as to what is intended and use an exact phrase rather than the word “annually” review. #3 - “within 12 months of the last . . . .” appears to be clearer than either of the others while #4 would provide a hard deadline that would not result in "date creep."
11.9	Dominion Resources Services, Inc.	Agree	Please see Dominion’s response to Question 9.
11.10	Reliability & Compliance Group	Agree	This could be better clarified. Some may interpret this to mean that procedures that address those topics will satisfy the requirement. A global definition of cyber security policy might help.
11.11	ISO New England Inc	Disagree	- Suggest changing the word “annually” to “a defined time frame” provided example at the end.- Suggest removing the “one or more formal” and add “documented and approved cyber security policies.”
11.12	Garland Power and Light	Disagree	* Please clarify the words "one or more" - does this require the review of all policies for the following functions
11.13	Consultant	Disagree	1. The list should include "Governance" as the first item. Suggest the first three items should be subheadings to the Governance item.2. Technically, R1 does not require designation of a CIP Senior Manager. As worded it requires a policy addressing the "Identification of a single senior management official...". Suggest an additional requirement statement requiring the Responsible Entities to designate a CIP Senior Manager, and document that designation.3. The mechanism for assigning responsibility is typically not a policy. Consider modifying the statement "Identification of a single senior management official with overall authority..." with "The senior management official's authority..." as an item to be addressed in the policy.
11.14	FEUS	Disagree	1.3 does not allow for delegation of authority for situations when the identified senior manager is unavailable. The Drafting Team should consider allowing a delegate or

#	Organization	Yes or No	Question 11 Comment
			alternative designated by the senior manager.
11.15	USACE HQ	Disagree	1.3 is missing the language that the single senior management official has the power to delegate some or all of the functions and/or actions to one or more named delegates. Also, double jeopardy is present since Requirements 6, 7, 11, 14, 15, 16, 17, 18, 20, 21, 23, 24, 25, 26, 27, 29, 30, and 32 cover part of or all of the policy documentation been required in 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11, 1.12, and 1.13.
11.16	Alliant Energy	Disagree	Alliant Energy agrees with EEI on verbiage suggestions and clarifications.
11.17	FirstEnergy Corporation	Disagree	As written the requirement and the list will require significant rework of existing policies for negligible benefit. In fact, the retraining that will be required will cause confusion and increase the challenge of achieving and maintaining compliance.Provide a standard that addresses all access issues (physical, logical, informational, etc.) instead of it being in multiple sections. Would also like to see emergencies being brought back into the main document, instead of having it part of each section.
11.18	Poplar Bluff Municipal Utilities	Disagree	Based on past experience, saying "Each Responsible Entity shall..." causes the Regional Entity to apply all CIP Standard requirements to all entities even if they own no Critical Cyber Assets. CIP-011 should clearly state that its requirements only apply to Entities that own BES Cyber Systems.
11.19	Con Edison of New York	Disagree	CIP-011-1 refers to timed requirements in various ways. The requirements should define the meaning and differences between annual, every year, within 3 calendar years, once every 12 months etc. There continues to be multiple interpretations of how within 365 days, within 12 months or in 2 calendar years, etc is defined.The term “annual” and “annually” should be defined. A suggested definition follows:Annual and Annually shall mean approximately every 12 months, but any period of no less than 9 and no more than 15 months.
11.20	E.ON U.S.	Disagree	CIP-011-1, R1.3 does not specify delegation by senior manager as currently permitted

#	Organization	Yes or No	Question 11 Comment
			under CIP-003-2. E ON U.S. proposes that delegation of authority by the senior manager be included as currently provided in CIP-003-2.
11.21	Dairyland Power Cooperative	Disagree	Communications between components/systems at different facilities or between different entities is an area lacking governance. Boundary protection is not sufficient.
11.22	ERCOT ISO	Disagree	Consider: “Each Responsible Entity shall develop, implement, approve, and annually review formally documented cyber security policies that address the following for its BES Cyber Systems:” Please clarify the meaning of “1.1. Applicability to organizational and third-party personnel”.
11.23	Progress Energy - Nuclear Generation	Disagree	Existing nuclear document hierarchy programs require review of policies, procedures, programs, and directives. The periodicity of the reviews should be consistent for nuclear generating facilities.See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
11.24	Southern Company	Disagree	For R1, What does “Addresses” mean? For 1.1...These are not usually actual third parties; the correct term is probably “non-employees acting on behalf of the Entity”.R1.3 and R3 create a requirement (a single responsible figure) that does not exist in any other NERC standard. Governance structures should be determined by the Entity and should not be regulated; the focus should be on the meeting of the other requirements and on the overall culture of compliance, so that the Entity can focus on creating the organizational structure that allows it to best meet the needs of CIP-011. This clause should be removed.Change the word "policy" in R1 to "policy or equivalent document".”Boundary protection” is undefined.
11.25	ReymannGroup, Inc.	Disagree	In many situations, outsourcing information technology tasks offers the Entity a cost effective alternative to in-house capabilities. Outsourcing, however, does not reduce the fundamental risks associated with information technology or the business lines or BES Systems that use it. Because the functions are performed by an organization outside the

#	Organization	Yes or No	Question 11 Comment
			Entity, the risks may be realized in a different manner than if the functions were inside the Entity resulting in the need for controls designed to monitor such risks. An additional security policy on 3rd Party Due Diligence and Vendor Management should be included. Functional Entities' should be required to establish a formal risk management processes to establish, manage, and monitor IT outsourcing relationships.
11.26	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	It is not clear what the Entity is responsible for if they do not own or operate any BES Cyber Systems. The assumption is not clear if the BES Cyber Systems list is null that Requirement R1 is then not applicable. Further, if a Low Impact BES Cyber System is the one and only System an Entity is responsible for, it is not clear whether a policy corresponding to an item (such as 1.5. Physical security) is required when the subsequent related Requirement pertaining to that item has a null listing for the Low Impact column in the following table (see Requirement R5). We advise the following change: "Each Responsible Entity who owns or operates one or more BES Cyber System shall develop, implement, and annually review formal, documented cyber security policies addressing applicability found in Requirements R2 through R32. The cyber security policies shall address each of the following categories, and include a statement of non-applicability for a category where appropriate:"
11.27	Western Area Power Administration	Disagree	It seems the requirement wants us to make the Physical Security Plan a part of the Cyber Security Policies? Is that what is intended?
11.28	Duke Energy	Disagree	List of topics need to be better defined. For example, 1.8. "boundary protection" may need to be changed to "electronic boundary protection". 1.9 should be changed to "Change Management" and "BES Cyber system maintenance" to "Configuration Management" for better alignment with NIST, COBIT and other control framework documents. Also, this policy is the only place where a Sr. Management official is mentioned. Does one or more imply a different policy per requirement or per business unit? If we have more than one policy, does the same Senior Manager need to manage and implement the requirements of the standard?

#	Organization	Yes or No	Question 11 Comment
11.29	NextEra Energy Corporate Compliance	Disagree	NextEra comments that during an emergency situation, a utility's primary objective is to end the emergency situations as soon as possible. For example, before, during and after the impact of a hurricane, the affected utility will mobilize much of its workforce to address system and customer restoration efforts. This may cause certain CIP requirements or deadlines to be missed for a short period of time. Moreover, there may be a need to relax CIP requirements, such as contractor qualification requirements for unescorted physical access into substations. Given the unforeseeable nature of emergencies, it is not possible to ensure all deadlines are met ahead of time, nor is it possible to pre-qualify all contractors, because it is not always known which contractors will be available or needed for emergency situations. A provision for emergency situations in the cyber security policy provides the utility and auditors alike with a framework and vehicle to ensure that any missed CIP deadlines or requirements that were relaxed are tracked, documented and that after the event, any missed or relaxed CIP requirements are addressed within a reasonable time after the emergency situation has ended. To implement emergency provisions and add clarity to other issues, NextEra proposes the following revisions:Each Responsible Entity shall have a documented cyber security policy related to the protection of BES Cyber System Components and BES Cyber Systems. The cyber security policy shall be reviewed every year during the month of March and updated, as necessary, no later than March 31st . The cyber security policy may also be updated as necessary. The cyber security policy shall include the following:B. The applicability of cyber security policy to employees and contractor personnel, including the manner in which the cyber security policy will be made available to employees and contractor personnel; C. The list of employees responsible for authorizing unescorted physical and/or cyber access to a BES Cyber System component consistent with R2-R4; D. The identification of a single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard, including contact information; E. A provision that addresses the Responsibility Entity's response to emergency circumstances in the context of CIP compliance. This provision shall address how the Responsibility Entity will track and document any missed CIP deadlines or CIP requirements held in abeyance

#	Organization	Yes or No	Question 11 Comment
			because of the emergency, and documents how, after the emergency condition has ended, any missed CIP deadlines or CIP requirements held in abeyance were brought back into compliance. An overview of the Responsibly Entity's approach to compliance is indicated with the following:
11.30	Ameren	Disagree	Overall this Requirement is vague and it will be open for interpretation during an audit. Suggest adding references to the corresponding requirements for sub-requirements R1.1 through R1.13. Also, if corporate policies cover all these areas would that be sufficient to prove compliance? Does the Senior Manager still need to approve this policy? These questions need to be answered to provide necessary clarity.
11.31	Tenaska	Disagree	R2 Clarify Sound Security PracticeR3 If a CCA were to go DOWN (NOT running) and the only vender that is available at that time that can fix it is not trained and/or criminal background and identity verified, does the standard address how to utilize the vendor and not violate the standard?
11.32	Exelon Corporation	Disagree	Requirement 1.3 should be revised to state a "Single Senior Management Official as per the entity's registration". Exelon is concerned that as presently written, Requirement 1.3 could be interpreted that Exelon as a corporate entity would need to have one and only one "single senior management official with overall authority and responsibility for leading and managing implementation of requirements within this standard".
11.33	Manitoba Hydro	Disagree	Requirement R1 states that each Responsible Entity shall "... annually review one or more .... cyber security policies..." which implies that a entity could review a single policy in a year. If an entity developed a policy for each of the R1 sub-requirements, it would take 13 years to complete the policy review. Consider including cross references to each of the specific Requirement numbers in 1.1 to 1.13.
11.34	Southern California Edison Company	Disagree	SCE first makes the following specific comments in relation to this Requirement: (1) R1.1 "third-party personnel" is vague and needs to be more clearly defined; (2) CIP-001-1-R1 does not include provisions for emergency situations; and (3) R1 appears to exceed the

#	Organization	Yes or No	Question 11 Comment
			mandates of FERC Order 706, paragraph 355, in that a finite list of topics to include in the policy were not required by FERC.In addition to those specific comments, SCE also makes the following general comment: the contained list attempts to be too prescriptive but does not seem to be exhaustive at the level of detail that is chosen. For instance, R1.5 and R1.6 are essentially sub-components of R1.8. Policy objectives should be such that they are at a higher level and yet clearly state the desired cyber security control objective in a manner that can drive the development of procedures and tools. The drafting team should consider dividing the standards into thematic areas that require policy statements for each thematic area.
11.35	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that the Requirement R1 in CIP-011 be re-worded to change the text “annually review formal documented cyber security policies” to "annually review a formal documented cyber security policy framework that includes policies, standards, and guidelines." Not everything within the framework would be a policy.
11.36	Independent Electricity System Operator	Disagree	See response to Q9.
11.37	Allegheny Energy Supply	Disagree	Suggested Revision:”Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:”Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.38	Allegheny Power	Disagree	Suggested Revision:”Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber

#	Organization	Yes or No	Question 11 Comment
			Systems:"Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.39	EEI	Disagree	Suggested Revision:"Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:"Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. EEI suggests additional language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. EEI suggests additional language to bring clarity or removing R1 1.8.It is unclear as to the distinction between "1.9. Configuration change management;" and "1.11. BES Cyber System maintenance;" EEI suggests additional language to bring clarity or removing R1 1.11.
11.40	Alberta Electric System Operator	Disagree	The AESO suggests removing "formal, " from the proposal as it is subjective.
11.41	APPA Task Force	Disagree	The APPA Task Force agrees with the intent, but believes the following improvements should be made:What does "formal" mean? Does the drafting team intend a Company-wide Policy?Terms used in later requirements ought to be defined hereTerms that are ambiguous, such as "Boundary protection" and "media sanitization" ought to have definition boxes associated with them. In general, definition boxes should be adjacent to the term as it is first used in the standard. Alternatively, a definitions sections such as is used in typical contracts could be a new standard section for those definitions that are used only in this standard that are not included in the Glossary.It should be clarified that

#	Organization	Yes or No	Question 11 Comment
			"Personnel ..." as used in 1.4 includes external contractors.1.7 seems to encompass 1.5, 1.6 and 1.8. Consider making 1.5, 1.6 and 1.8 sub-bullets of 1.7The APPA Task Force believes that a number of the requirements listed in the tables throughout CIP-011 should be part of an overarching policy developed by each registered entity. While each utility's approach may be different, each registered entity should establish a coherent approach to cyber-security for its BES facilities. Requirement R1 should be viewed as the cornerstone of defining what is important to that utility. We believe the subsections of R1 are confusing and need clarification. Since revocation of access is common to many of the requirements The APPA Task Force believes the following Additional/Edited cyber security policies should be addressed in each entity's policy:1.2.1 Revocation of Access - Triggering Criteria
11.42	Southwestern Power Administration	Disagree	The phrase "leading and managing" is too restrictive, particularly for larger entities whose single Senior Management Official may have overall authority and responsibility, but his or her managers are the personnel who are responsible for leading and managing the details of the cyber program.1.3 Identification of a single senior management official with overall authority and responsibility for implementation of requirements within this standard;
11.43	Kansas City Power & Light	Disagree	The requirements here for a policy statement are much too prescriptive and are unnecessary. Policy statements should be global and encompassing and provide overall guidance. Recommend removal of a policy statement requirement from this proposed Standard. What purpose does this requirement serve or problem does this requirement solve? If this requirement is not included, what process or procedure will not be done in support of the remainder of the requirements? What is important are the processes and procedures that are in place to support the meat of the Standard. Mandatory and enforceable requirements are sufficient to stand alone. If a company feels they need a policy statement to support the CIP Standards, or any other Standard, let that be their decision.Do not agree with the need for requirement 1.3 regarding the need to appoint a single senior management official for overall authority and responsibility for leading and managing implementation of the CIP requirements. These requirements cover a broad

#	Organization	Yes or No	Question 11 Comment
			spectrum of systems and can engage many organizational parts of a company that one person may not be meaningful over all parts. NERC Reliability Standards compliance is sufficient weight to allow a company to determine the level of approval it needs to achieve and ensure compliance throughout an organization for CIP and any other NERC Reliability Standard.This Standard should focus on identification of cyber systems that need protection and an appropriate level of protection needed and move away from requirements that manage an organization such as R1.
11.44	LCEC	Disagree	The requirements of a formal policy should be defined.Boundary protection should be definedmedia sanitization should be definedCyber Security incident should be defined
11.45	Progress Energy (non-Nuclear)	Disagree	The term annual needs to be defined. Is it during a year, per 12 months, Jan 1 to Jan 1, 365 days, from what starting date, etc.R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.46	Michigan Public Power Agency	Disagree	The term annually is not consistently applied throughout the industry. For some organizations, this term means sometime in a calendar year, others apply it to their fiscal years. Some have applied it to mean a 12 month period based on the last event. The term either needs to be defined similarly to R3, where there is a local definitions box or the wording should be altered to remove the ambiguity.
11.47	US Bureau of Reclamation	Disagree	There are 6 "definitions" provided in CIP-011 which are needed to enforce the standards. Those 6 "definitions" need to be formally proposed as definitions in order to ensure enforceability of the standard.
11.48	Southwest Power Pool Regional Entity	Disagree	This requirement is not objectively auditable as written. Some level of explanation or direction needs to be defined to assist the entity and the auditor in a common

#	Organization	Yes or No	Question 11 Comment
			understanding of the expectation. While a simple regurgitation of the applicable enumerated (not "R") requirements is undesirable, the required polic(ies) need to state expectations in sufficient detail for the entity and its contract / vendor support personnel to understand the requirements of the policy as they pertain to implementing the standard(s).
11.49	American Municipal Power	Disagree	This requirement seems to be too prescriptive.
11.50	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
11.51	We Energies	Disagree	We Energies agrees with EEI: Suggested Revision:"Each Responsible Entity shall develop, implement, and annually review, documented cyber security policies that address the following for its BES Cyber Systems:"We Energies agrees with EEI: Suggested Revision for R1 1.3:Identification of a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to requirements within this standard; R1 1.7: System security; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.7.R1 1.8: Boundary protection; is unclear as to meaning or intent. Suggest addition of language to bring clarity or removing R1 1.8.It is unclear as to the distinction between 1.9. Configuration change management; and 1.11. BES Cyber System maintenance; Suggest addition of language to bring clarity or removing R1 1.11.
11.52	American Electric Power	Disagree	What burden of proof is needed for items 1.4-1.13 to demonstrate implementation? Would this be the same proof that would be required to prove R2-R32 have been met? Is this an instance of double jeopardy? Failure to meet an item in R2 would also mean failure to implement the cyber security policy in R1. Suggest removing "implement" and allowing the R2-R32 requirements stand as proof of implementation.To what level of detail must the cyber security policy address the items? Is it sufficient to outline how they will be addressed? Different auditors may have different levels of detail in mind. Is this meant to outline a Responsible Entities Cyber Security Policy? The majority of the

#	Organization	Yes or No	Question 11 Comment
			details for compliance will be found in the procedures, not in policy statements. Does this do anything more than demonstrate a Cyber Security culture for a Responsible Entity?
11.53	ReliabilityFirst Staff	Disagree	What does the term “addresses” in Requirement R1 mean? How does an entity “address” sub-requirements 1.1 through 1.13? Sub-requirement 1.3 needs clarification regarding the definition of the phrase “single senior management official”. Does this phrase mean one individual for an enterprise or one individual for each registered function, or either?
11.54	WECC	Disagree	While we agree with the general proposal and list, this requirement should be rewritten to more clearly indicate what is required. The word formal should be defined in this context. The level of detail required in the policies should be indicated. Suggest changing review annually to "review at least every 365 days" or to "once during the calendar year" depending on what SDT's intent is for the requirement.(1.1) The phrase,” Organizational and third-party”, is inconsistent with phrases used in other requirements. Consider utilizing the same language used to describe individuals with access to cyber systems, or simply state “everybody”. (1.3) No specific documentation is required.(1.4 through 1.13) These requirements are very vague and offer no guidance at all as to the level at which these topics must be addressed. As written this requirement provides no value whatsoever, and is essentially unauditable.
11.55	Verizon Business	Disagree	1) Revise 1.9 Configuration Change Management to two separate lines – one for “Change Management” (which would apply to procedure compliance, etc.) and one for “Configuration Management. 2) The list is too vague. The prior approach with CIP-003 identifying the specific policies needed is preferable. 3) Item 1.8, “Boundary Protection” should be defined. The requirement should state whether it is consistent with the definition in NIST 800-53. 4) Revise 1.5 to read “Physical Security of BES Cyber System Components.”

12. Requirements R2 to R4 of draft CIP-011-1 concern personnel training, awareness, and risk assessment, which were previously contained in CIP-004. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Note: CIP-011-1 R2 through R4 now resides in CIP-004-5 R1 through R3.

Several commenters suggested training related to networking, hardware, software, and electronic interconnectivity was either unnecessary or inappropriately targeted to individuals who have no working knowledge of the subject. The SDT agrees, and has made the training 'role-appropriate'; meaning only individuals whose roles necessitate such knowledge must receive the training.

Some commenters suggested the awareness requirements were not clear; specifically, use of the terms "proper use", "essential", and "sound security practice" were highly subjective. In response, the SDT has removed those terms and provided a requirement that can be audited more objectively.

In addition, some commenters suggested the quarterly reinforcement timeframe was too frequent. However, the SDT believes the requirement to update security awareness material is not overly burdensome and serves the reliability benefit of getting up-to-date threat information to a wide audience of individuals who can protect the BES Cyber Systems.

Some commenters suggested the annual timeframe for training individuals was inflexible and should allow for additional time to have individuals trained. The SDT agrees and has suggested the alternative use of the phrase "at least once every calendar year, but not to exceed 15 months between training."

Some commenters suggested the requirement for photographic identification was not necessary, since it adds the additional requirement for individuals to be on site for a personnel risk assessment. In response, the SDT acknowledges the requirement for photographic identification would necessitate individuals to be physically present. However, the requirement has been modified to require identity verification only for the initial personnel risk assessment performed for each individual.

Some commenters also suggested background checks were overly burdensome by requiring entities to cover all of the locations of residents within the past seven years. The SDT appreciates these comments but does not feel an adequate personnel risk assessment can be made without such information.

#	Organization	Yes or No	Question 12 Comment
12.1	Alliant Energy		Alliant Energy agrees with EEI to strike "sound" and "essential from R2. Also, additional

#	Organization	Yes or No	Question 12 Comment
			clarity around awareness training and the term “provide” and whether that requires completion tracking. Suggestion: Use the term “distribute” instead of “provide” to remove that implied obligation for awareness training.Additionally, R3.2 is not a practical requirement. Role based training is good; however, training should be specific to the responsibilities within the BES Cyber System and should not be prescribed by the standard. What is “specified” and why is training on networking hardware and connectivity required for users/operators of BES Cyber System Components who are not network administrators. What benefit is provided by providing technical training to personnel whose core competency and job duties do not require this level of expertise or understanding?R3.5 introduces a rolling creeping calendar. Recommend changing all 12 month timeframes to either 13 calendar months or 5 calendar quarters from the previous completion to allow entities to maintain a program with an annual training rollout with the appropriate amount of lead time to be successful in annual renewal. A 12 month timeframe will create a training program that becomes administered on a user by user, day by day basis without considerations for consistent annual content updates and bulk annual renewal.R4.1 is too prescriptive and does not take into consideration personnel with access and zero need for onsite presence.
12.2	National Rural Electric Cooperative Association (NRECA)		In R4, other than performing, documenting and updating personnel risk assessments, is there anything else that is required regarding personnel risk assessments? It does not appear there is, but wanted your confirmation on that.In R4.3, please specify what "at least once every seven years" means. This needs to be made clear so there are no misunderstandings. For example, if the last assessment was done on Jan. 15, 2001, does this provision mean the next one must be completed by Jan. 15, 2008?In R4.3, if a person never had an assessment completed and they already has access to BES Cyber Systems, when must the initial assessment be completed?
12.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R2The phrase “to ensure that personnel maintain awareness ...” should be removed from the requirement as it adds ambiguity to the requirement. Is the auditor going to measure “quarterly reinforcement” or “personnel ... awareness” or both? It

#	Organization	Yes or No	Question 12 Comment
			seems like the drafting team is trying to add an objective for the requirement. If that is the case, then consider one of two other alternatives: (1) adopt International Standards Organization format where they have an objective for each requirement introducing each requirement; or (2) develop a longer Purpose section where the purpose of each of the requirements is further embellished. This comment should be carried on to all of the requirements.What does “reinforcement” mean?R3The term “granted authorized ... access” seems to be superfluous. Authorizing and granting are two different activities and the standard seems to prohibit granting access without first authorizing access (unless under certain specified exceptions). Consider just using the term “granted” in this requirement. The confusion between the terms “granted” and “authorized” is throughout the document and ought to be clarified.Consider correlating the training requirements in R3 with whether the person is a “user” or “administrator”, and whether the training is “job training”, a “refresher”, or “awareness”, with separate levels of training frequency and content for each of these categories.3.1 should not include “procedures” since these procedures are not identified elsewhere in the standard. The word “program” should be struck from “Visitor control program” since nowhere else in the standard is there a requirement for such a program. There should be no “back-door” requirements for procedures or programs such as these.3.5 should use the term “annually” instead of “at least once every twelve months” to give entities flexibility around various business needs on when during the calendar year to hold training flexible.R4The term “granted authorized” is superfluousConsider shortening “ensure a personnel risk assessment is performed” to “perform a personnel risk assessment”
12.4	Regulatory Compliance	Agree	R2 - Awareness - please clarify what are accetable forms of awareness.R3.2 - suggestion - STRIKE the reference to networking hardware and softwareR4 - Question: How do you propose to close the gap in regards to a criminal background check of an employee who has lived outside the country for a period of time in the past seven years that may not equal the 6 month period but long enough to be involved in supicious activities?
12.5	Emerson Process	Agree	R2 and R3 do not have tables for their applicability to three impact-types of BES cyber systems. Would it be better to include the tables for consistency with the rest of the

#	Organization	Yes or No	Question 12 Comment
	Management		standard?
12.6	Northeast Utilities	Agree	Recommend that R2 be clarified to indicate whether or not documentation must be provided that awareness material was received and understood by the CIP authorized personnel.Also, it is recommended that more guidance is provided on the level of training expected under R3.2 when stating "include training on networking hardware and software and other issues of electronic interconnectivity". The clarification is important to acknowledge that the intent is clearly not to have all personnel with electronic access to any BES Cyber System to become network engineers. For example: for operations personnel, what is the level of knowledge expected concerning networking hardware and software?
12.7	Green Country Energy	Agree	Will their be any guidance, footnotes or would ANY cyber security training be acceptable?
12.8	Independent Electricity System Operator	Disagree	- Suggest changing R3.2 so that it is only required based on personnel having a role in networks, etc. An operator and other personnel do not need to know how a firewall or switch works or its software. They may need to know how to use their token for t
12.9	Reliability & Compliance Group	Disagree	: "Sound security practices" is too vague of a term. How is this going to be audited? Who will determine what a sound security practice is? There needs to be an industry standard used. Is it going to be security practices listed under NIST 800-53? What about physical security practices? Without a benchmark, how can we measure adherence to the standard?R3 is way too cumbersome the way it is written. Keep the first part of the standard written the way it is. Then start a new sentence that says, "exceptions to this requirement must be specifically outlined in the responsible entities policies and are limited to emergency situations and acceptable alternative training." The part of the standard that reads, "impact the reliability of the BES or emergency response, to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems" is just confusing to read and understand. No matter what is done, try and make this requirement more than one sentence.R3 is better than the old

#	Organization	Yes or No	Question 12 Comment
			standard in how it defines how training should be handled for different roles and responsibilities. The 12 month timeframe needs to be tightened down even further. Is that 12 months +/- one month or is it every 365 days?
12.10	USACE - Omaha Anchor	Disagree	3.2 - should be worded closer to 3.3. or 3.4. You are giving training on network hardware and electronic connectivity to everyone with electronic access. This is counterintuitive - these folks for the most part do not have a need to know. They should only be given as much information as necessary to do their job.
12.11	Luminant	Disagree	3.5 We would prefer that training be conducted annually (completed within a calendar year) to avoid the confusion of tracking multiple comliance dates. How much documentation must be maintained? 12 months? 24 months, 36?
12.12	Platte River Power Authority	Disagree	Access to “any BES Cyber System” shouldn’t automatically require training on networking hardware and software or other issues of electronic interconnectivity. The training should be tailored to the individual’s job junction and not based on the BES Cyber System they have access to. For example, an operator doesn’t need to know the brand, model, configuration, or connectivity of the networking hardware that they’re using. They need only know the proper use of the asset they’ve been granted access to. I would like to avoid training individuals on the interworkings of our network when they have only been granted limited electronic access.
12.13	Liberty Electric Power, LLC	Disagree	CIP-011 R2 requires quarterly training for all plant personnel in cyber security. This is too frequent, and I would suggest changing to annual.CIP-011 R4.3 repeats the error of CIP-004 concerning the word “update”. There were many comments about requiring entities to have their long-time employees provide government-issued ID every “update” in the RFI, and the recordkeeping and potential for violation over trivia continues by not addressing the issue. I suggest changing the wording to define update as doing the background check again, and not getting into the realm of potential violations over lost wallets.

#	Organization	Yes or No	Question 12 Comment
12.14	E.ON U.S.	Disagree	CIP-011-1, R3.5 unnecessarily inhibits an organization's flexibility by mandating training every 12 months. E ON U.S. proposes that the Standard state "annual training", as currently required.CIP-011-1, R4 contains requirement of the Personnel Risk Assessment that should be revised. When seeking information from foreign nations concerning someone having resided in those foreign nations, compliance with these literal requirements may not be possible or feasible. An exception should be included to address a failure to obtain this level of evidence following a good faith attempt to do so.CIP-011-1, R4.3 ignores practical problems with requiring background checks of contractors and/or service vendors. Privacy concerns have raised many questions as to whether literal compliance is possible (especially in the context of this Standard which eliminates some of the language from the former CIP-004). E ON U.S. proposes that the requirement provided by the Regional Compliance Implementation Group ("RCIG") in RCIG-A-002 be adopted conceptually in this Standard.
12.15	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
12.16	LADWP	Disagree	Consultants or employees who lived abroad for a time may not be able to meet the 4.1 requirement to cover all locations where subject has resided. This could prevent proper authorization to BES systems.
12.17	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes Personnel Training, Awareness, and Risk Assessment should only apply to personnel with access to high impact BES cyber systems and not include personnel with access to medium and low impact systems. CenterPoint Energy also suggests changing R3.2 to: "For personnel having job duties that require a role in BES Cyber System networking and electronic interconnectivity, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems."Numbering of sub-requirements for R3 and R4 conflicts with numbering of requirements in Tables R3 and R4 (there are two 3.1 and 3.2 and two 4.1 and 4.2).

#	Organization	Yes or No	Question 12 Comment
			CenterPoint Energy suggests moving all sub-requirements for R3 and R4 to tables to be consistent with other sections in CIP-011.
12.18	FEUS	Disagree	Disagree with Comments: 3.2 requires personnel with electronic access to have training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems. Extensive training on networking hardware and software should be limited to support staff or personnel with administrative privileges. It is not clear what 'other issues of electronic interconnectivity' is?3.5 requires training to be conducted every 12 months from the date of 'initial' training. The Drafting Team should consider revising the wording to allow for training more frequent to align with a regular training schedule for more personnel.4.1 requires a seven year criminal history check covering all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more. How would the Responsible Entity verify 'all locations' were identified by the subject for the criminal history check? If a subject is attending an out-of-area school via online courses it is not logical to perform a criminal background check for the location of the school.
12.19	Southern Company	Disagree	For R2, This requires the Entity to either track which personnel have access to every low-impact system or to include all personnel company-wide, including vendors and contractors, in the awareness program. A table should be added excluding low-impact Cyber Systems to parallel R3 and R4.For R3, How does "granted authorized electronic access" interact with the situation where a network service on a system is available to anyone who can get a packet to it? For 3.5, A specified 12-month cycle makes the training program much more difficult to administer without any benefit to reliability. A 14-month cycle would allow a reasonable annual training program to work.3.2 does not actually address any security need for the large majority of personnel with access. While Order 706 requires that NERC address the issue, that FERC requirement could be considered to have been met by the standards comment process without the wording making it into the final standard.Suggested rewrite of R3: Each Responsible Entity shall ensure that all personnel who are granted authorized electronic access and/or

#	Organization	Yes or No	Question 12 Comment
			authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training, when specified in CIP-011-1 Table R3 - Cyber Security Training, prior to their being granted authorized access in order to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.Temporary authorized access may be granted for specified exceptional circumstances that are approved by the senior management official identified in Requirement R1.3 or their documented delegate; for circumstances that require temporary access for emergency response; or for circumstances that would otherwise negatively impact the reliability of the BES. Suggested rewrite of R4: Each Responsible Entity shall ensure that all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, undergo a personnel risk assessment, when specified in CIP-011-1 Table R4 - Personnel Risk Assessment, prior to their being granted authorized access in order to ensure that personnel have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements.Temporary authorized access may be granted, without prior personnel risk assessment, for specified exceptional circumstances that are approved by the senior management official identified in Requirement R1.3 or their documented delegate; for circumstances that require temporary access for emergency response; or for circumstances that would otherwise negatively impact the reliability of the BES. R4 is difficult to implement for the case of vendor support through remote access and for vendor support staff who are not citizens of the US, Canada, or Mexico.
12.20	Progress Energy (non-Nuclear)	Disagree	For R3 - the definitions in the box should be included as formal definitions. It is confusing with these text boxes hanging with only certain R#s.R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words.For 3.1 - cyber training included incorrectly here...last bullet. Move to 3.2.4.1 First bullet comments- this new requirement appears to be a duplication of the E-Verify/I-9 process in which employment eligibility is verified for all new hires. All employers are required to verify their employees’ employment authorization and confirm that the identification documents presented are legitimate, thus establishing an individual’s identity covering

#	Organization	Yes or No	Question 12 Comment
			both the employee and contractor population. Additional verification through the PRA or requiring completion of the PRA after completion of the employment eligibility requirements adds additional steps to the process with no added value.4.1 Second bullet comments - the current regulation requires a 7 year criminal check. It does not specify that the check needs to cover everywhere the person worked or went to school and lived for > 6 months. The new language appears to be taken from a response to the interpretation given to the Army Corp of Engineers by NERC regarding how a PRA should be performed, which PE disagrees with.The current wording requires companies to gather much more data on an individual from the individual (as that is the only source of the information). Not even Nuclear attempts to gather this kind of data (everywhere worked and went to school for > 6 months) when they perform their checks. Based on historical experience, for those who have had multiple employments the information provided by the individual with regard to employment will likely not be accurate.PE suggests running a 7 year criminal history on all addresses that show up on the application or in the credit databases and then running a nationwide search to cover any other areas. An alternate to that may be fingerprint checks if utilities can be given access to the data.Either of these approaches will streamline the process.CIP-011-1 R3.1 (Cyber Security Training) - It appears that R3.1 was written with the intention of providing a level of training appropriate to job functions (language which was explicitly in previous versions) in regard to those with only unescorted physical access (such as janitors, electricians, HVAC technicians, etc); however the last bullet point 'Identification and reporting of a Cyber Security Incident' could easily be misinterpreted to be requiring training of a cyber nature rather than those of a physical nature directed against cyber assets (which I believe is the training we should be providing an individual with the aforementioned responsibilities)
12.21	Alberta Electric System Operator	Disagree	For R3.1, consider removing "and storage media" from bullet "The proper handling of BES Cyber Systems information and storage media" because information handling should be implemented regardless of the media type.For R4.1, consider changing the seven year time horizon, and make time horizon dependent on BES Cyber System impact level. For example, Low Impact could be seven years, Medium Impact five years, and High Impact

#	Organization	Yes or No	Question 12 Comment
			three years.
12.22	American Municipal Power	Disagree	I agree with the intent, but I feel there is some redundancy between requirements for training, awareness, risk assessment, etc. that should be addressed more concisely (less requirements)
12.23	GE Energy	Disagree	i) R3.2 lists a requirement for training on networking hardware for all users having electronic access. Perhaps this should only be for users with administrative access to network hardware. If this requirement is really calling out the need for VPN or similar training, this should be more specific than "network hardware".ii) Is it possible for vendors' personnel risk assessment process and records to be ratified/certified by NERC, so that individual Responsible Entities do not have to duplicate the effort for those vendors who have teams providing services to multiple REs? This would be more efficient and secure.iii) Vendor privacy issues are a concern regarding the background screens. Some clarity on the expectation between the client and vendor and the paperwork required to validate a screen, and clarity on who should actually conduct the screens would be helpful (client versus vendor). The expectation should be for the vendor to maintain their own records.
12.24	Public Service Enterprise Group companies	Disagree	In CIP v1~v3 the requirement for refresher training was "Annual", where "Annual" was understood to mean sometime within a calendar year. The new requirement of "once every 12 months from the date of initial training" implies that a daily checks are required for each person that had previously been training on whether training has expired. This imposes undue administrative overheard on Registered Entities without significantly enhancing cyber security. More flexibility is needed to accommodate vacations, illness, etc. One possibility is that training is required annually, with an up to 90 day extension for good cause or administrative efficiency.
12.25	National Grid	Disagree	In R2, National Grid recommends an annual reinforcement.Recommend that R3.2, R3.3 and R3.4 change "training" to "role appropriate training"

#	Organization	Yes or No	Question 12 Comment
12.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
12.27	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggested revision:R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words. Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site? Make requirement for photo ID apply to physical access only.
12.28	Minnesota Power	Disagree	Minnesota Power requests that the Standards Drafting Team consider replacing the phrase “provide all” with “make available to all,” in order to ensure clarity and avoid the potential that this phrase may be interpreted to include the requirement to document that the materials were actually received by all personnel. For example, it would be difficult to document that bulletin board postings were “provided” to each individual employee.Regarding Requirement R2, “...under their security awareness program to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems” Minnesota Power has the following comments: o What security awareness program is being referenced? The Standard does not require the creation or implementation of a security awareness program. Minnesota Power recommends removing “under their security awareness program” from the Requirement. o What are “the cyber security practices that are essential?” The way this is stated infers that there is a known list of essential practices, which are particular to BES Cyber Systems (as opposed to general IT security practices), though none are referenced. Regarding Requirement R3, Minnesota Power recommends rewording the purpose statement as follows:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to access being authorized as specified in CIP-011-1 Table R3 - Cyber Security Training. This training is required except in exceptional circumstances that are approved by the single senior management official or their authorized delegate and

#	Organization	Yes or No	Question 12 Comment
			impact the reliability of the BES or emergency response." In addition, Minnesota Power has the following comments regarding Requirement R3: o R3 makes reference to a delegate for the senior management official, however R1 does not allow for the ability to assign a delegate for any purpose. o The box of definitions for R3 includes definitions for "routable protocol" and "non-routable protocol" however; these definitions are not used in R3 and therefore should be removed. o Sub-section 3.1 references a visitor control program which is not defined anywhere in this requirement. In light of the Standards Drafting Teams intentions to remove the "how-to" components of these Requirements, Minnesota Power recommends removing references such as this to a "program" and replacing with a statement such as "How visitor access is managed." o Regarding sub-sections 3.2, 3.3 and 3.4, as these sub-sections are currently written, it is not clear that this training is required for those individual's with a "need to know" only. o Regarding sub-section 3.2, what is the word "specified" in "specified electronic access" referring to? Minnesota Power recommends removing this term from the phrase as it doesn't add to the meaning of the sentence. o Regarding sub-section 3.2, "training on the networking hardware and software and other issues of electronic interconnectivity" is overly broad and could be interpreted as in-depth technical training, which would go beyond the intent of this Requirement. Minnesota Power recommends the following alternate wording, "training on the cyber security policies, access controls and procedures for the BES Cyber Systems to which they have electronic access." o For sub-sections 3.3 and 3.4, Minnesota Power recommends adding a comma following "...BES Cyber System recovery," for 3.3 and "...BES Cyber System incident response," for 3.4. o Regarding sub-section 3.5, the term "This" at the beginning of the sentence should be replaced with "Each" to be consistent with the other Requirements. o Minnesota Power recommends adding a statement to Requirement 3 that the training referenced in subsections 3.1 through 3.4 can be performed in a single training session or in multiple training sessions each covering one or more of the required topics. Regarding Requirement R4, Minnesota Power recommends rewording the purpose statement as follows:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems,

#	Organization	Yes or No	Question 12 Comment
			including contractors and service vendors, have undergone a personnel risk assessment prior to access being granted as specified in CIP-011-1 Table R4 - Personnel Risk Assessment. The completion of this assessment is required except in exceptional circumstances that are approved by the single senior management official or their authorized delegate and impact the reliability of the BES or emergency response. This is to ensure that personnel who have such access have been assessed for risk, subject to existing collective bargaining unit agreements, in accordance with federal, state, provincial, and local laws."In addition, Minnesota Power has the following comments regarding Requirement R4: o Regarding sub-section 4.1, the use of the phrase "personnel risk assessment program" seems inaccurate. Rather, 4.1 only defines what a personnel risk assessment itself shall, at a minimum, include. Minnesota Power recommends that the term "program" be removed from this sub-section as it's not required to demonstrate compliance. o The addition of "via photographic identification documentation issued by a government agency" to sub-section 4.1 could create an unnecessary burden on Registered Entities, especially for those vendors and contractors who do not come on-site. Minnesota Power recommends utilizing the language of the current CIP-004-2 Standard and requiring SSN verification for U.S. residents and photographic identification documentation for non-U.S. residents. o In the event that Standards Drafting Team chooses to leave the language of sub-section 4.1 as is, Minnesota Power recommends that photographic verification of identity be done at the time of initial access and that it is not necessary to renew this verification every 7 years. o Regarding sub-section 4.2, what does "document the results" mean? Under the current NERC CIP-002 - CIP-009 Standards there has been some confusion regarding what a Registered Entity needs to show compliance with this type of Requirement. Does this mean keep a redacted copy of the personnel risk assessment or would logging a summary of the results (e.g., "no findings"), including dates, source of background check, etc., be adequate? The Standards Drafting Team should consider clarifying what is meant by "document the results" so that consistency can be established.
12.29	NextEra Energy Corporate	Disagree	NextEra believes that the former standard provided valuable examples of awareness training methods which should be part of this revised standard. One question that arises

#	Organization	Yes or No	Question 12 Comment
	Compliance		is how will the delivery of this awareness training be measured? The standard should clarify the requirement. Also, the standard should provide examples of exceptional circumstances under which exception from training and PRA requirements may be documented.
12.30	Garland Power and Light	Disagree	o Disagree or need clarification with 3.1 - 1st bullet "The proper use of BES Cyber Systems" What does "use" mean - The EMS control system is operated by NERC certified operators and updated / maintained by qualified technical personnel. For CIP training, what is meant by train on the "use" of this system o Clarification on 3.2 should apply only to personnel having a role specific to support services for "networking hardware, and software and other issues of electronic interconnectivity supporting the operation and control of the BES cyber systems" and should be limited to security features. Training of all personnel in these areas will reduce cyber security.
12.31	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggested revision:R2 contains two very subjective words: "sound" and "essential." Suggest striking these words. Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site? Make requirement for photo ID apply to physical access only.
12.32	Kansas City Power & Light	Disagree	Quarterly reinforcement is excessive and places an unnecessary administrative burden on Regional Entities and a poor investment of time and effort distracting from the productive work of maintaining cyber system security and integrity. Annual training is sufficient for the FERC Standards of Conduct, for important reliability functions in the EOP Standards such as black start and energy capacity emergencies, and for CIP sabotage recognition and reporting. Annual training for the personnel with access to identified cyber systems is sufficient to ensure the importance of maintaining the security and operation of identified cyber systems.R3.2 requires training that is much too detailed for personnel with access to a cyber system. Would this make sense for someone whose task was to wire in a Remote Terminal Unit for acquisition of field data into an EMS? The training specified in requirement R3.1 is sufficient for these kinds of

#	Organization	Yes or No	Question 12 Comment
			personnel. Recommend removal of R3.2.R3.5: Requiring annual cyber security training 12 months "from the date of initial training" is an unnecessary burden on the Regional Entity. It is enough provide for an annual training within a calendar year for those personnel who have physical and electronic access to cyber systems. What issue is this addressing? It is more important to focus investments of time, energy, and finances toward the actual security and integrity of the cyber systems than to support an administrative system to ensure training is done at a specific time rather than the training itself.R4.1 is too prescriptive in specifying the actions that are required to achieve the background check objectives. There may be other regulatory restrictions that prevent adherence to the prescription described here. Recommend removal of such prescription and include the language from CIP-004-2 that states to perform such checks "as permitted by law and subject to existing collective bargaining unit agreements".
12.33	Con Edison of New York	Disagree	Quarterly training is excessive for the large number of people likely to be involved. This training should be annual or at maximum twice a year. This training will get very expensive given the large number of people to be added to the training pool.
12.34	Dominion Resources Services, Inc.	Disagree	R2 - Based on the SDT's comments at the workshop, the intention of the Awareness program is not to require documentation of security awareness at an individual level. This interpretation is evidenced by the differentiation between the intent of security awareness versus the intent of security training. As defined in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program", awareness is not training. The purpose of awareness is to focus attention on security. Many of the techniques commonly used to deliver security awareness topics (e.g., posters) do not lend themselves to tracking at an individual level. On one hand, awareness topics are intended to allow individuals to recognize IT security concerns and respond accordingly and, on the other hand, training strives to produce relevant and needed security skills and competencies. The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus attention on an issue or set

#	Organization	Yes or No	Question 12 Comment
			of issues. Consequently, the SDT's intentions are correct and consistent with industry best practices. Given that the intent of this requirement is to reinforce cyber security program expectations for those personnel with access to BES Cyber Systems and not to document evidence of individual training, the following alternate wording is proposed: "Each Responsible Entity shall establish a security awareness program. The program shall provide for reinforcement, at least quarterly, on selected topics of security expectations and practices required to ensure the protection of BES Cyber Systems." 3.2 - Requirement R3.2 proposes training personnel who have electronic access to a BES Cyber System "on the networking hardware and software and other issues of electronic connectivity supporting the operation and control of BES Cyber Systems." Dominion recognizes that networking and network transport mechanisms (i.e., connectivity) involve specialized skills requiring a high level of expertise and experience. Because of the specialized nature of networking, providing this training would provide only a very limited security benefit at best, and could encourage personnel without the full qualifications and experience necessary, to take actions affecting network connectivity that would adversely impact the reliability of the BES. Based on Paragraph 434 of the Directives in FERC's Order No. 706, the Commission's intent was only that training programs encompass this training, not that any individual who has electronic access to a BES Cyber System receive such training. This requirement should be removed.3.5 - The change from annual to 12 months appeared to cause some confusion at the workshop and does not provide for a grace period (e.g., 12 months plus or minus a month to allow for shift workers and emergencies). Dominion requests that the SDT consider returning to using "Annual" and define how annual is to be used for these standards. Dominion prefers that "Annual" be defined as "12 months plus or minus a month" since this provides some flexibility in completing the task and also allows the Responsible Entity to not be forced into 11 month cycles so as not to miss a 12 month deadline. For example, Dominion had a training session set up for certain field personnel. The night before the meeting, a storm came through the system and caused enough damage that the meeting had to be cancelled because everyone was needed for restoration activities. The logistics involved in setting up these training sessions are often complex and a grace

#	Organization	Yes or No	Question 12 Comment
			period would provide the flexibility for rescheduling without compromising the spirit or intent of the training objective. Dominion understands that the "12 months plus or minus a month" definition is being used throughout the nuclear industry. Dominion suggests the following alternate wording for R3.5:"Initial training shall be conducted prior to granting access to BES Cyber Systems. Re-training shall be conducted annually."R3.5 contains requirements that are not identified in Table R3. All requirements should be contained within the associated table. Please see Dominion's response to Question 9. 4.1 - With inclusion of the nuclear plants, time horizons for personnel risk assessments are shorter than currently required by the standard. For example, Nuclear does background checks for unescorted access authorization every 5 years. Since they are done every 5 years, they do not check history for the last 7 years. To accommodate this difference, which effectively exceeds the requirements of this standard, it is recommended that the language in the 2nd bullet of R4.1 be revised to read:R4.1 o A criminal history records check initially and at least every 7 years thereafter, covering all locations where, during the time from the last check to the current time, the subject has resided . . .
12.35	Southwestern Power Administration	Disagree	R2 - Replace "shall provide" with "shall make available to" to clarify that the Responsible Entity must make quarterly awareness available, and not document that all personnel have reviewed and understand the awareness material.R3 & R4 - what would be an exceptional circumstance that would warrant training exception and/or investigative exception from the senior manager for personnel who are granted authorized electronic access and/or authorized unescorted physical access? If this is where the SDT is attempting to replace the previous "Exception to Policy" requirement, the placement of that language in R2 and R4 may need to be revisited, as these requirements seem to focus only on managing controls for personnel that DO have authorized access rights - not emergency personnel or non-authorized personnel access in emergency situations.R3.2 - This requirement is ambiguous in its inclusion of the phrase "other issues of electronic interconnectivity" A better approach would be to list the minimum coverage or topics to be covered. R3.5 - The requirement can be interpreted to read that everyone with authorized access will have to be trained exactly 12 months from his or

#	Organization	Yes or No	Question 12 Comment
			her initial training date. This would cause the responsible entity to be continually training and tracking staggered dates and creates an overly burdensome documentation effort, leading to the opportunity for mistakes and missed course deadlines. It is much more efficient and advantageous to do annual training in a group format. A better approach would be to state: "The Responsible Entity shall maintain documentation that such cyber security training is provided or offered once every 12 months, and documentation that personnel having authorized electronic access and/or authorized physical access to BES Cyber Systems have completed such training within 60 calendar days of such training being offered."
12.36	Ameren	Disagree	R2 - Without examples of what minimally constitutes reinforcement, this requirement will be problematic to audit. Would oral reinforcement count and how would you document that? Give examples such as posters, emails, events, or meetings would at least give an indication of the need to document evidence of the reinforcement taking place. A quarterly review seems extensive and an administrative burden. Once or twice per year should be sufficient.â€,â€,The bullets under R3.1 and R4.1 should be numbered as sub-requirements so that they can be cross referenced for audit purposes, i.e. R3.1.1 or R4.1.1 etc. Using the same numbering in the tables and in the requirements is confusing. The tables should use letters or roman numerals so they would not be confused with the sub-requirements indexing.
12.37	EEI	Disagree	R2 contains two very subjective words: "sound" and "essential." EEI suggests striking these words.For R2, This requires the Entity to either track which personnel have access to every low-impact system or to include all personnel company-wide, including vendors and contractors, in the awareness program. A table should be added excluding low-impact Cyber Systems to parallel R3 and R4.
12.38	Allegheny Energy Supply	Disagree	R2 contains two very subjective words: "sound" and "essential." Suggest striking these words.

#	Organization	Yes or No	Question 12 Comment
12.39	Allegheny Power	Disagree	R2 contains two very subjective words: “sound” and “essential.” Suggest striking these words.
12.40	Constellation Power Source Generation	Disagree	R2 states quarterly reinforcement in sound security practices under their security awareness program. This may be training, but it does not have to be, as stated in the CIP V4 Workshop. However, this requirement as written does not seem to be auditable. How can an entity prove that an email/screensaver/poster/meeting meets the reinforcement stated in the requirement? Further clarity is needed, either within the requirement or in a guidance document.
12.41	Madison Gas and Electric Company	Disagree	R2, We would propose replacing the terms “provide all” with “make available to all”, as we are concerned the word “provide” could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were “provided” to each individual employee.Within R3 and R4 there is an exception of “except for program specified exceptional circumstances “ that is modified with the phrase “and impact the reliability of the BES or emergency response” (R3 only), please clarify. Is this exception giving the single senior manager the ability to wave cyber security training in the event that a non trained person is required to accomplish a task that they alone have the skill set for completion of said task (ie, a software engineer associated with the company that designed your SCADA system)?R3.1, The first bullet states “The proper use of BES Cyber Systems” and should be deleted since that is assumed as stated within the actual requirements of R3.1. The intent should be that training should be focused on protection of the BES Cyber System not how the particular BES Cyber System works, Please clarify.R3.2, The word “specified” is used and is not understood. Please clarify. If this is to mean additional training outside of the training within R3, than please “specify” that the entity shall have additional training program (module) for “specified” training that is not covered by R3. Please clarify if this is the required training differences between users and system administrators?The following requirements do not include a table of Low Impact, Medium Impact and High Impact (where the word “required” is

#	Organization	Yes or No	Question 12 Comment
			used under each column):R2R3.3R3.4R3.5R4.3Is this to indicate that all Entities must comply with these requirements whether or not they have BES Cyber Systems? Please clarify?
12.42	LCEC	Disagree	R2. The reliability benefit statement should not be included within the requirement section. This would be better positioned under the purpose section of the standard where it does not add confusion to the specific requirements that are being audited. The ISO27001 standards include an "objective" statement for each set of security controls which adds clarity and serves as a good best practice example.What is meant by reinforcement? How will this be demonstrated to an auditor?What is meant by sound security best practices? How will this be demonstrated to an auditor?R3 Remove or rewrite all content in the first paragraph after Table R3 - Cyber Security Training. The intent of this is unclear and very confusing.Split performance and program requirements into separate requirements for ease of auditing. If there is a requirement to have a program it should reside in its own requirement. Ref bullet 3 3.1Personnel with electronic access need to have an understanding of the risk associated with interconnectivity not necessarily the specific hardware involved. Personnel with the ability to change hardware configurations should have an understanding of hardware, software and interconnectivity impact.Training requirements should be tailored to user versus administrator and job based versus.The table should include the full range of requirements, like Table R5, and if not applicable should explicitly state that, not through blank cells. This leads entities to interpret that no training is required for these systems.4.2 in the table R4 should read unescorted physical access.
12.43	US Army Corps of Engineers, Omaha Distirc	Disagree	R2. meaning of quarterly reinforcement is vauge seems like it could be difficult to maintain audit records. 3.2 All users with electronic access do not need to know or understand networking hardware and software. Such information is usualy limited to those who support the network/system and have a need to know.
12.44	CWLP Electric Transmission, Distribution	Disagree	R2. Quarterly reinforcement training of cyber security practices seems excessive. This could be reduced to an annual obligation consistent with the training obligation in

#	Organization	Yes or No	Question 12 Comment
	and Operations Department		requirement 3.5. R3.2. This appears to require training on all systems connected to the BES, not just the specific system a user may require access to. A user accessing a server, PC or relay should not require training on network devices such as switches, routers, etc. This should be limited to requiring training on the specific area of the BES Cyber system the user is utilizing. R3.3. Similar to R3.2 this requirement should provide wording specifying that the training obligation is limited to the specific role the user has in regards to the Cyber System. R4. Requires a definition of “Electronic Access”.
12.45	Consultant	Disagree	R2. Suggest deleting the word "all" as redundant.R2. Suggest deleting the words "practices under their security awareness program". The requirement should be for dissemination of security information, not to create a program.R2. Change the words "that are essential to" to "associated with". Essential is a subjective term.R2 - R3 This is an example of where the insertion of 'local definitions' makes reading the requirement text difficult. Also, "For the purpose of this standard" is unnecessary and essentially not true. If the term is defined in the standard it is expected to be included in the next update to the NERC glossary, as that is how terms get in the glossary.General Comment- the term "and/or" is bad grammar. The word "or" is all that is necessary.R3 - Suggest deleting the word "all" as it is not consistent with the requirements identified in Table R3.R3 - This is three requirements and an objective statement stuffed into one convoluted sentence.R3[-1] shall ensure personnel complete training prior to be being granted access as required in the Table.R3[-2] personnel under this requirement includes employees, contractors, and service vendors.R3[-3] Designated CIP Senior Manager shall approve instances where exceptional circumstances related to BES reliability or emergency situations may allow access without completed training.R3[-4] cyber security training objective is to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.-- Suggest rewriting as individual requirements for better clarity.R3.2 Suggest deleting "specified" as an unnecessary word.R3.2 Suggest deleting "any" as it is not consistent with the requirements in Table R3. Training is not required for "any" access, only for those systems identified.R3.2 Suggest specifying the training is for the security aspects of "networking hardware and software and other issues of electronic interconnectivity" not training on installation,

#	Organization	Yes or No	Question 12 Comment
			programming, or other aspects of these components.R4 - Suggest deleting the word "all" as it is not consistent with the requirements identified in Table R4.R4 - This is three requirements and an objective statement stuffed into one convoluted sentence.R4[-1] shall ensure a personnel risk assessment is performed prior to be being granted access as required in the Table.R4[-2] personnel under this requirement includes employees, contractors, and service vendors.R4[-3] Designated CIP Senior Manager shall approve instances where exceptional circumstances related to BES reliability or emergency situations may allow access without a completed personnel risk assessment.R4[-4] cyber security training objective is to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.Suggest rewriting as individual requirements for better clarity.R4 - "assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements." The personnel risk assessment is not performed in accordance with "federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements". It is performed in accordance with the Registered Entitie's policies and procedures, and should be in compliance with "federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements." Suggest modifying the wording of to clarify.Wording between R3 and R4 is inconsistent. R3 - completed security training & R4 - personnel risk assessment is performed. Suggest consistent wording as completed security training & completed personnel risk assessment. R4.1 suggest deleting the word "program" as unnecessary. It is the personnel risk assessment that has the specified identity check & background checkLogically, the topic in R3 should precede R2. It would seem to make more sense to grant access prior to providing security awareness on that access.Likewise, the topic R3.4 should precede R3.3. It would seem to make more sense to respond to an incident prior to recovery from an incident.Clarify annual for review of the policies, and for training. Suggest using the regulatory basis of over 30 years from the nuclear industry in dealing with periodicity for defining these periodic timelines. Should probably be a definition in both new standards to relate to periodic requirements.

#	Organization	Yes or No	Question 12 Comment
12.46	Western Area Power Administration	Disagree	R2: Please clarify whether "all personnel" includes "contractors and service vendors".R2: Please clarify what is meant by "reinforcement" required quarterly.R2: Needs some language clarifying intent. Does authorized electronic access = unescorted physical access? If so, this has major ramifications for support.R3: Requires the Responsible Entity to ensure that contractors and service vendors complete cyber security training - it does not specify that they must complete OUR training, just that they can provide proof of training that includes the specifics of R3.1. Is this the correct intent?R3.2: This requirement is too vague. What training on networking hardware and software are required? Is the intent to have training on the various forms of electronic access (VPN, dial-up, direct connection to equipment with a laptop or other diagnostic tool, etc.)? Is it directed at users like dispatchers who connect to the system via a console or workstation? All of the above? Each category of electronic access would have different training requirements.R3.3: Does this requirement specifically relate to disaster recovery/COOP/Business Resumption Plan? Would it also include training for field staff doing repairs on specific systems? Will we have to document all of the training they receive, including training on the maintenance and repair of all substation electronic equipment?R4: What is the definition of “program specified exceptional circumstances”? R4.1: Why are we changing to photographic versus finger printing? Photographic is easily fooled.R4.1: Would an entity be responsible for maintaining the results of a 7 year criminal check for outside entities having physical access (foreign utility workers, vendors, contractors, etc.)? If the other entity is also a NERC defined CIP applicable entity, is verification by that entity that the employee is properly vetted satisfactory? This is sensitive information that other entities may not be able to divulge due to local, state or national laws.
12.47	Southwest Power Pool Regional Entity	Disagree	R3 and its included requirements should be clarified to require training appropriate to the roles and responsibilities of the recipients. It is likely inappropriate to train a janitor or security guard with physical-only access on the proper use of BES Cyber Systems the same way a person with electronic access would be trained. Similarly, it is likely unnecessary to train a vendor support staff with only remote electronic access on the

#	Organization	Yes or No	Question 12 Comment
			physical access controls and visitor control program. 3.2 requires training for personnel having "specified" electronic access. What is "specified" electronic access? Additionally, it is likely not appropriate to train a dispatcher/operator on networking hardware, software, and connectivity issues, although they have electronic access. Greater granularity or assignment of responsibilities to roles may be necessary. 3.5: is the 12-month requirement a hard 12 months? Or is there some grace period permitted, such as +/- one month, to avoid calendar creep? And, does the 12-month timer reset with the completion of the latest training received or is the expectation that the training is actually performed approximately the same time every year regardless of any training that might be completed at a different time of the year? Additionally, rather than specifying the "date of training" shall be documented, consider using language similar to "[t]he responsible entity shall maintain documentation demonstrating that the required cyber security training is completed at least once every 12 months." Let the entity determine what is necessary to demonstrate compliance. R3 Overall, consider requiring a minimum expectation as to the quality of training. For example, should there be some sort of post-training assessment to determine if the recipient understands the course material? 4.3: Consider clarifying the requirement to "...update each personnel risk assessment within seven years of the previous personnel risk assessment" and make it clear that in this instance the requirement is from the actual date of the previous personnel risk assessment, not "in the same calendar year" or "+ / - some grace period."
12.48	The United Illuminating Co	Disagree	R3. Introduction is a run-on sentence with clauses nested within it. It is unduly confusing. I would reword for the SDT, but I can not understand the clausa relationships.R3.1 to R 3.4: There are employees who will require training in 3.1 thru 3.4. This amount of training could cover multiple days separated by periods of time. The requirement does not allow for General training on one day, Vyber incident response with the response team on another day, and training in backup restoration with a third team on a different day. R3.2: What specified electronic access triggers this requirement? Electronic access is not synonymous with remote electronic access, so what is being directed with this requirement. A user with a password does not require these topics. R 3.5 annual training from the initial date of training is too restrictive.

#	Organization	Yes or No	Question 12 Comment
			Union workforces are trained in groups and training schedules shift from year to year. Also a new union higher may receive an initial one-on-one training session and then be synchronized with the rest of the workforce by repeating the training in under 12 months.Suggest “once every 12 months from the date of the initial training, or the last completed training date” This will allow flexibility to reset the training date without going over the 12 months between training classes.Also request the SDT consider allowing a two month grace period in the requirement. UI suggests including a requirement for venors/contractors who provide support via remote access only (EMS/SCADA vendors). These vendors do not require training in physical access control procedures, or visitor control processes. Additionally, they often service multiple organizations and should not be required to view the same cyber security program as the BES cyner system owner employees. The suggested wording is:”For personnel requiring electronic access only training shall include at a minimum:- The proper use of BES Cyber Systems o The proper handling of BES Cyber Systems information o Identification and reporting of a Cyber Security Incident
12.49	Black Hills Corporation	Disagree	R3.1 & R3.2 does not allow for role-based training. Need to have unique numbering between sub-requirement and table references. (There should only be one 3.1 in R3)
12.50	Detroit Edison	Disagree	R3.2 requires “training on the networking hardware and software and other issues of electronic interconnectivity”. Training system operators on network gear is beyond the scope of their job duties. At the Dallas workshop, the drafting team stated that this training was required by FERC order 706 paragraph 434. That paragraph also says “we clarify that our proposal discussion on this topic was not intended to suggest that personnel have training that is not appropriate for an employee’s duties, functions, experience, or access level”. We don’t believe that FERC is requesting all personnel be trained on network gear, only that the training is appropriate to the person’s job functions. System administrators and network engineers would need to have training on the network, operations personnel do not.R3.2 also requires training prior to access of any BES Cyber System which is inconsistent with table entry 3.1 which does not require training for Low Impact or Medium Impact with routable connectivity.R3.5 removes the

#	Organization	Yes or No	Question 12 Comment
			term “annual” that was used in CIP-004 and replaces it with once every 12 months. This is too restrictive. Consider an entity that has a window for training in the month of May. Requiring every 12 months would cause the calendar to creep earlier in the year so eventually the training would be moved to April. We prefer “at least once per calendar year, not to exceed 14 months between instances”. The identity verification via photographic identification required in R4.1 is too prescriptive. The standard should be the “what” not the “how”. Previous versions of CIP-004 required an identity verification with the example of SSN verification. Consider changing the first bullet to “Identity verification (e.g., Social Security Number verification in the U.S. or via photographic identification documentation issued by a government agency i.e. Federal, State or Provincial)”.Table 4.2 should only require a PRA for unescorted physical access.
12.51	SCE&G	Disagree	R3.5 12 months should be changed to annually to allow entities to utilize a "calendar year" to setup training pools to conduct the necessary CIP training. Otherwise provisions should be made to allow initial training to be conducted during the implementation period of the standard.R4 SDT should consider allowing entities to leverage PRA controls in place (i.e. Nuclear PRA process)SDT should develop requirements for entities to validate a vendor's/contractor's PRA process. This would impose the burden of conducting the administrative work for the PRAs on the contractors/vendors, while still maintaining the compliance burden with the entity.
12.52	Powersouth Energy Cooperative	Disagree	R3.5 Suggest additional consideration be given to the requirement “every 12 months from the date of initial training.” Suggest the following wording: “no later than the end of the calendar month that the 12 month anniversary of the individual’s initial or previous training falls in” or similar to extend the window to a reasonable time to allow training to be done in a schedule fashion to allow some leeway for unanticipated delays that could previously lead to non-compliance due to a hard deadline. R4. Request additional language be added to clarify the allowance of reciprocity of PRA’s between a contractor or vendor and the responsible entity. It is understood that PRA’s are an important component of proper security but due to the volume of contractors and vendors used at any given time, a mechanism for the third party to perform their own

#	Organization	Yes or No	Question 12 Comment
			PRA and provide assurance that the PRA meets the requirements of the registered entity in both substance and time requirements will reduce cost and complexity greatly.
12.53	American Electric Power	Disagree	R3: In regards to "are approved by the single senior management official identified in Requirement R1 or their delegate and...", does this statement add any benefit to security? Is a senior manager or delegate's approval needed each time an emergency situation is declared?3.2, 3.3, 3.4: This is an attempt at role based training. Would it be better to combine 3.2, 3.3, and 3.4 together into a single requirement? Suggested wording: "The cyber security training must be role based for personnel that are users, administrators, responsible for system recovery, and responsible for responding to or investigating cyber security incidents of BES Cyber Systems."3.5: Regarding "conducted at least once every 12 months from the date of initial training", will this result in a date backup? Does an entity need to keep the initial date of training for all users? Does it seem feasible to still have the initial training records 20 years down the road?If training is completed on 6/30/2011, would it need to be completed before 6/30/2012? If it was then completed on 4/15/2012 would the next date of training be before 6/30/2013 or before 4/15/2013?Suggested wording: "at least once every 12 months from the last completed training date".
12.54	ISO New England Inc	Disagree	Recommend rephrasing R3 so that is clear that the Entity does not need to list all potential emergency responseTraining should be on policy, procedures, standards, and process and how to conduct oneself. Training should not be on networking,hardware,software. Companies have personnel that have the background in each function that are subject matter experts. That is there job and should not need to be trained each year on it since that's what they do every day. For R3 there is a sub requirement 3.2 and then another requirement in table 3 numbered 3.2 this can confusing.R3.2 in table 3 please defined what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?For R4 there is a sub requirement 4.2 and then another requirement in table 4 numbered 4.2 this can confusing.R4.2 in table 4 please defined what is meant by external connectivity. External to BES Cyber

#	Organization	Yes or No	Question 12 Comment
			System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?The term "annual" should be replaced with the phrase: "no fewer than X (e.g. 9) months, but no greater than Y (e.g. 18) months". The time duration in "X" and "Y" should be clarified by the Standard Drafting Team, taking into consideration the appropriate level of exposure the time duration would provide. This phrase would provide Registered Entities with flexibility within any given calendar year to accomplish the prescribed action, but at the same time restrict companies from taking action in December of one calendar year, and then again in January of the next. This should be done to all the section that have 12 months. Scenario...In 2010, we roll out the training on June 1.Person A, who has access to CCAs, completes the training on June 15. In 2011, we roll the training out again on June 1.Person A, who has access to CCAs, completes the training on June 25. Under the new language, it could be interpreted that Person A has been out of compliance for 10 days if access was not revoked.The following are items we have in our training today, that will become requirements under the new standard: o Visitor control program (R3.3.1) o Identification and reporting of a Cyber Security Incident required(R3.3.1) o Recovery - note, this was required, but the language is more specific here (R3.3.3)The following are new requirements that will impact the training programs: o Training on networking hardware and software and other issues of electronic interconnectivity (R3.3.2) o BES Cyber System incident response action plans and procedures (R3.3.4)
12.55	Hydro One	Disagree	Recommend rephrasing R3 so that it is clear that the Entity does not need to list all potential emergency responses.We were wondering if the intent of R3.2 is to prevent access to a launch point for a multi location attack. (i.e. why limit the physical access to only sites with external connectivity?)
12.56	Northeast Power Coordinating Council	Disagree	Recommend rephrasing R3 so that it is clear that the Entity does not need to list all potential emergency responses.Recommend that R3.2, R3.3 and R3.4 change "training" to "role appropriate training".

#	Organization	Yes or No	Question 12 Comment
12.57	ERCOT ISO	Disagree	Recommend the following be more clearly stated as an exception: “except for program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response”. R3.1: Consider: This cyber security training shall cover these requirements as well as policies, access controls, and procedures developed for the BES Cyber Systems, and include, at a minimum, the following required items: R3.2. Please clarify the intent of “training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems”. Examples of curriculum would help. R3.5. The requirement does not address retaining records of completion of initial training. R4: Recommend that “except for program specified exceptional circumstances that impact the reliability of the BES or emergency response” be addressed more clearly as an exception.R4.2. Consider: “Each Responsible Entity shall document the results and review of each personnel risk assessment.”
12.58	ReliabilityFirst Staff	Disagree	ReliabilityFirst is not clear on the meaning of the phrase “. . . except for program specified exceptional circumstances that are approved by the single senior management official. . .” If this is intended to cover the language of CIP-003 Requirement R1.1 referring to, “. . . including provision for emergency situations.” we believe the proposed language needs more clarity. In Requirement R3.1, the use of the word “specified” is unclear as to the intent of this requirement. We believe the drafting team should add language to clearly express the intent of this requirement and, more importantly, the intent of the word “specified”. Regarding Requirement R3.5, please provide guidance on the phrase, “once every 12 months”. For example, if an individual is trained on December 1st one year, can the individual receive the training on December 12th the following year and still be in compliance? Regarding R2, there is no documentation of implementation required, making auditing of the requirement impossible. A requirement to document the quarterly reinforcement is needed. Also regarding R2, a “security awareness program” is mentioned, but not required here or elsewhere and should be added.

#	Organization	Yes or No	Question 12 Comment
12.59	Constellation Energy Control and Dispatch, LLC	Disagree	Remove the phrase "sound security practices" or identify and define what the phrase means, i.e. sound security practices as defined in the cyber security policies.
12.60	BGE	Disagree	Remove the verbiage “sound security practices” or identify and define what this means.
12.61	US Bureau of Reclamation	Disagree	Requirement 2: Agree, but requirement should emphasize Program first then quarterly awareness refreshers.Requirement 3: AgreeRequirement 3.1: Agree, but revise "at a minimum" to "in addition" in the introductory statement.Requirement 3.2: Disagree. The requirement for network training should not be applied to everyone with logical (electronic) access, only to those who administer network and/or system administration. As written, this requirement could be taken to apply to operations staff (operators) with access to operations consoles. They do not need network training. Further, what is "specified network access." Requirement 3.3: Agree. Role-based training is probably a good idea, but this might be handled with a general statement.Requirement 3.4: Agree, see above.Requirement 3.5: Agree, but there should be some tolerance so that there is no date creep.Requirement 3 (in Table): The requirements R3 and R4 include tables which are in themselves requirements. Since the numbering system is the same as other requirements, this could result in confusion with what the actual requirements are. It is suggested that Tables R3 and R4 be clarified.Requirement 4: This requirement needs to be simplified. It is wordy and confusing.Requirement 4.1: The requirement should not limit identification processes to photographic means. Fingerprints are and should be acceptable. Further, the criminal check requirement, with local information, is beyond what can normally be addressed. Suggest this check be limited to a national level only. The risk assessment process needs to specify that an adjudication process needs to be completed.Requirements 4.2 and 4.3: Agree.
12.62	Network & Security Technologies Inc	Disagree	Requirement 3.2 (training on networking hardware and software), as written, seems to require that ALL personnel with electronic access to BES Cyber Systems receive such training. This frankly makes no sense. Will SCADA/EMS operators be expected to understand the intricacies of Cisco IOS? Furthermore, it violates the principal of “need to

#	Organization	Yes or No	Question 12 Comment
			know." Suggest this requirement be reworded in a manner that makes it similar to 3.3 and 3.4 and limits its scope to personnel responsible for hardware and software.
12.63	Oncor Electric Delivery LLC	Disagree	Requirement 3.2 is not appropriately worded. Most users with electronic access to our Cyber Systems have no need to know anything about the networking hardware, software, or interconnectivity issues. The personnel responsible for maintaining this equipment may need additional training but most have required skill sets as specified by their job descriptions.Requirement R4.2 uses the term "results" of a Personnel Risk Assessment. Different auditors may interpret this term differently. We propose this to be a binary result, ie pass/fail and stated as such, for clarity.
12.64	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Requirement R2 has all BES Cyber System operators to have a security awareness program that will maintain cyber security practices. However Requirement R3, R5 and R6 exempt Low Impact BES Cyber Systems. How can an Entity begin a security awareness program where Initial training (R3) and physical security (R5 & R6) is not required? This is very confusing.
12.65	San Diego Gas and Electric Co.	Disagree	Requirements 3.2 - 3.4 in CIP-011-1 seem to imply that a Registered Entity must have a separate training program for these three subjects. Unless the requirement is intended to be that prescriptive, SDG&E recommends a single training requirement that addresses the requirements in R3.1 - 3.4. This will help make the training requirements more manageable.Attempting to split hairs between training requirements for physical and cyber access to BES Cyber Systems for Medium and High Impact systems seems to unnecessarily increase risk exposure for a Registered Entity and complicates the process and controls needed to meet R3 and R4 of CIP-011-1.
12.66	Southern California Edison Company	Disagree	SCE requests clarification on the scope of R3.1. This requirement requires people listed on Table 5 (those with physical or electronic access to "high impact BES system[s]" to receive training on the "proper use of the BES cyber system". This requirement as currently written is unclear whether the training requirement only applies to people who work with affected systems, or whether the requirement more broadly applies to

#	Organization	Yes or No	Question 12 Comment
			everyone who is permitted unescorted physical access to a PSP. If it is the former, then SCE believes that would be the correct application of this rule. However, if it is the latter case, then persons who are granted unescorted physical access rights to a PSP, but who do not themselves operate these systems (for example, CIP-cleared security guards), would have to receive training on the "proper use" of the protected system. Such training should only be required of individuals who actually work with protected systems, and not to everyone who has unescorted physical access rights to a PSP.SCE also seeks clarification on Requirement R2. As written, R2 requires quarterly "reinforcement". The drafting team should clarify the distinction they imply by using the term "reinforcement" rather than "training" as used in R3. Finally, SCE ask for clarity on Requirement R3. As written, Requirement R3 seems to allow for exceptions in the training requirement. The drafting team should clarify why an "organizational infeasibility" is being allowed while a structured method to seek technical feasibility exceptions is being eliminated. Both conditions create a situation where strict compliance with the standard is impossible to implement.
12.67	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
12.68	Idaho Power Company	Disagree	Sub requirement 3.2 is too broad. Dispatcher/operating personnel who have electronic access via an EMS application would not need training on networking hardware and software but it would be appropriate for EMS support staff. Cyber security incident identification and reporting would be sufficient for Dispatch/Operations personnel.
12.69	APPA Task Force	Disagree	The APPA Task Force agrees with the changes proposed by MRO-NSRS to replace "provide all" with "make available to all." We also believe the term "reinforcement" is not a defined term and should be replaced with "awareness material." As stated in our response to question 11 above, it is important to reference the required policies under requirement R1.If the drafting team does not follow Objective format suggested in response to Question 10, the APPA Task Force recommends the following format:R2.

#	Organization	Yes or No	Question 12 Comment
			Objective:Personnel Training, Awareness, and Risk Assessment: To ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems. R2. Requirement:Each Responsible Entity shall make available to all personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems at least quarterly awareness material in sound security practices under their security awareness program. The security awareness program will be part of the policy developed under requirement R1.The APPA Task Force cautions the drafting team on using the terms “grant” and “authorize” interchangeably. The following is our recommended revision to R3 with the Objective removed from the requirement:R3. Objective:To ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems.R3. Requirement:Each Responsible Entity shall ensure all personnel who are granted electronic access and/or unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being authorized access when specified in CIP-011-1 Table R3 - Cyber Security Training, except for program specified exceptional circumstances that are approved authorized by the single senior management official identified in Requirement R1 or his/her delegateR4. Objective:To ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. R4. Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted electronic access and/or unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being authorized access when called for in CIP-011-1 Table R4 - Personnel Risk Assessment, except for program specified exceptional circumstances that impact the reliability of the BES or emergency response,
12.70	Indeck Energy Services, Inc	Disagree	The definition of Cyber System is so broad that these requirements are applied on a one size fits all basis. A control center computer system requires a different level of requirement than a substation RTU. This lends itself to differentiating the standards by function and/or functional entity. R3.2 applies IT networking requirements on the operator who logs in to use the functionality, without any ability to program it. The term

#	Organization	Yes or No	Question 12 Comment
			"specified electronic access" is overly broad.
12.71	Manitoba Hydro	Disagree	The meaning of "quarterly reinforcement" is unclear. Consider whether Requirement R3.5 should refer to "Each Responsible Entity", rather than "This Responsible Entity". Requirement R4 appears to be missing the explicit requirement that access would be prohibited based on the negative or poor results of a personnel risk assessment; it just speaks of a personnel risk assessment being required. The structure of Requirement R3 and Requirement R4 is confusing and needs to be corrected. As written, the Table CIP-011-1 R3 applies to each of the sub-requirements, which may not meet the intent of the requirement - how does Table 3 item 3.2 for physical access relate to Requirement 3.2 for electronic access? What does "specified" mean in Requirement 3.2? The duplicate use of the same numbering of the requirements and the table items is very confusing. The format of requirements together with the use of tables for R2 to R4 should be consistent with the rest of the proposed standard. Manitoba Hydro agrees that cyber security training is not a standard requirement for all personnel who have unauthorized physical access to Low Impact BES Cyber Systems, and therefore is not auditable. We do not agree that training is not a requirement for personnel who have authorized electronic access to Low Impact BES Cyber Systems, and suggest that it be an auditable requirement.
12.72	WECC	Disagree	The new way these requirements are written is very confusing. Too many levels, sub-levels, bullets and tabled criteria. Please simplify. Consider replacing with a requirement for Training and Awareness program that addresses the criteria that the SDT feels is critical for security and reliable operation of BES Cyber Systems.Regarding the phrase, "all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors", consistent language should be used through the standards. It may be useful to create a term for this group of people, define it, and use it in place of this long phrase.The last half of the requirement sentence lacks clarity. It is difficult to understand what is being required. If the intent is to create an exception process for training, the text should be removed. Standards should not have exceptions written into

#	Organization	Yes or No	Question 12 Comment
			them; they should establish a high bar of excellence.(3.1) “Visitor control program” needs definition or explanation.(3.2) The training requirements in this sub requirement seem vague.(3.3) Regarding the reference to “Systems;” most controls apply at the device level, and therefore should be required at that level.(3.5) Time intervals need to be clearer and well defined.(Table R3) Why no training for low impact systems? Seems arbitrary.
12.73	Bonneville Power Administration	Disagree	The objectives of these requirements (“to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems,” “to ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems,” and “to ensure that personnel who have such access have been assessed for risk, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.R3: Exception is somewhat confusing. In particular, is "or emergency response" an alternative to "...are approved by..."? In other words, it could be read that exceptional circumstances require either approval or an emergency. However, it could also be that the "or emergency response" is an alternative to "impact the reliability..." It appears that the former is more likely, but the reader should not have to parse the sentence to get there. Some selected bulleting would help.Suggested rewrite of R3:Recommended Changes - Objective 3 - To ensure that personnel are aware of the policies, access controls, and procedures in place to protect BES Cyber Systems. R3. The Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, have completed cyber security training prior to their being granted authorized access when specified in CIP-011-1 Table R3 - Cyber Security Training, except for - Program specified exceptional circumstances that are approved by the single senior management official identified in Requirement R1 or their delegate and impact the

#	Organization	Yes or No	Question 12 Comment
			reliability of the BES, or - Emergency responseThis assumes the first interpretation of "or"3.1 is acceptable3.2 Needs clarification, as it is not clear what the intent is. In a non control center environment, persons who have electronic access to BES Cyber Systems often do not have nor require knowledge or training in networking hardware and software. They make electronic connections and use their electronic access to collect electrical system information such as fault data, monitor device functions or do electrical systems analysis. It is not their job to understand networking.R3.3 and R3.4 are acceptable.R3.5 requires that training be conducted, but does not specifically require that every individual complete it. Also, it addresses the first annual training, but doesn't clearly stated what to do afterwards. The intent seems to be that each person complete training within each year. In other words, if the initial training was on July 1 2010, then training would be needed sometime in 2011 (say September), some time in 2012 (January?) and so forth. As currently written, a separate 12-month clock would be needed for each person. Finally, it's not clear if the required documentation is for the initial training, the annual training, or both. The SDT should be very specific as to what it means for how frequently an individual must take cyber security training. Suggested rewrite: Rewrite 3.5 to address annual training only: "This Responsible Entity shall ensure that all such persons receive annual training at least once each calendar year, starting the calendar year after they are granted access. The Responsible Entity shall remove authorized access from any individual who fails to complete such training in a timely manner." This removes some flexibility from the entities, but produces an unambiguous and manageable annual training program.We believe that a new requirement, 3.6, is needed to address documentation: "This Responsible Entity shall maintain documentation of any cyber training addressed in R3 or its subrequirements, includinge the date the individual's training in completed."Header in Table R3: Doesn't address annual training: Suggest "Cyber Security Training is Required Prior to Obtaining and For Continued:"R4: Has the same issue with the intent of "or emergency response" that R3 has. We suggest the same solution.The way that R 3.5 is written, it appears that two things must be done: the Responsible Entity must maintain documentation and each individual who is required to take cyber security training must take it as specified.

#	Organization	Yes or No	Question 12 Comment
			Would a violation of R 3.5 be due to an organization not maintaining documentation or due to an individual not having taken the required cyber security training in a timely manner? Or could there be two violations of R 3.5 - one for an organization not having up-to-date documentation and one (or many) for an individual(s) not having taken the required cyber security training in a timely manner? There is no indication in R 3.5 what should happen if an individual does not take the cyber security training as and when required. Should that individual's electronic access and/or unescorted physical access be revoked until the cyber security training has been completed? Or is what is important here only that the documentation be maintained regardless of whether each individual takes the cyber security training as and when required?For large organizations with a thousand or more people that must take cyber security training, is it possible that R 3.5 could indicate those organizations can provide the cyber security training during specific times of the year (say within a 3-month window) without regard for each individual having to take the training at a specific time? In this case, there would be no violation in an individual did not take the training exactly 12 months apart (or whatever the time requirement is) if the individual took the training within the 3-month window in each of two years.
12.74	Exelon Corporation	Disagree	The quarterly reinforcement requirement as spelled out in CIP-004 R1 Versions 1 through 3 is more specific and should be continued into this version. Requirement 3.2 as currently stated could cause someone such as a control room operator using an EMS system to be required to receive training on networking hardware and software for which they have no business need to know. It also could impact job specific training that is focused on improving reliable operations, due to the loss of precious training time being used for training that is not required for their position. We would suggest including wording such as "....appropriate to personnel roles and responsibilities"Requirement 4.1 second bullet states that "a seven year criminal history check" be performed. It is not clear from the requirement as to what agencies would need to be contacted to accomplish such a check. If local Police agencies are envisioned to be part of this check, that does not seem to be a very practical approach. R4. The need to show a photo ID is unnecessary to ensure a valid Identity Verification. The methods currently used to cross

#	Organization	Yes or No	Question 12 Comment
			reference and verify identity are satisfactory. To now require photo identification provides no additional benefit but would make it extremely difficult for remote personnel since we would now need someone to personally view the original photographic document. This would eliminate the ability to electronically transmit the required information.
12.75	Duke Energy	Disagree	The reinforcement requirement in R2 is vague and is up for interpretation by auditors. The Responsible Entity should only have to prove that the reinforcement information is provided. Previously, various means to provide the information, including posters, etc. were acceptable. This should still be the case. If so, is should not be necessary to prove that all personnel read the poster. R2 is open to interpretation as to what kind of evidence is sufficient. Explicitly state that materials are sufficient. Explicitly state which levels of Impact apply to R2. Need clarification on the program exception in R3. Does this apply to electronic and physical access? Must every situation need to be accounted for in the program or may it be case-by-case? Also, Requirement R3 contains a run-on sentence that makes the requirement hard to understand. Please consider breaking this into 2 or more smaller sentences.Requirement R3.2: What is meant by "specified electronic access?" Also, the requirement is vague in that it can be interpreted that the user of a BES cyber system needs detailed networking hardware and software training, when this is not the case. The user typically needs to know that device A is connected to device B and needs to know how to use the software. Said user does not need to know that the network communication routes through a brand XYZ switch using Ethernet and that the software was written in C# and so on. Clarification needed for audits, etc.Requirement R3.3: This requirement also needs bounds. If Employee A has a role in the recovery of BES Cyber System 123 only, then Employee A needs training on action plans and procedures to cover only BES Cyber System 123.R3.4 seems to be incomplete.Requirement R3.5: Is there any grace period on the 12 months? If there were "exceptional circumstances" such as in R4? For example, what if Technician A was due for training in June and was called for emergency storm duty and missed the training as a result? For 4.1, who will keep track of photographic identification? What is BA/TOP doing for Areva evidence of photo IDs? Will we have to gather the photo ID every 7

#	Organization	Yes or No	Question 12 Comment
			years? Suggest changing 4.3 to only include the criminal history check.
12.76	Nuclear Energy Institute	Disagree	The use of the expression "authorized electronic access" should be clarified, in all requirements in this standard where used. The correct expression should be "authorized electronic administrative access." Users who have access but no authorization to perform administrative functions on a BES Cyber System Component are of greatly less concern than those individuals having administrative access. Performing, as required by R4.1 a seven year background check, on each individual with non-administrative access to a Component is inappropriate. The focus should be on individuals who would pose a direct challenge to the system's reliable operation. An alternate solution may be to define "authorized electronic access" in the "Definitions" section.
12.77	FirstEnergy Corporation	Disagree	Though role based training is appealing, this activity is difficult to manage and maintain. It becomes administratively difficult to develop, maintain and track different training programs. A better approach would be having training that is differentiated by access (e.g. logical vs. physical.)For R3.2 qualifications should be made for only those people responsible for supporting networking hardware and software. There is no valid reason to provide networking training to non-networking personnel.If 3.3 and for 3.4 remain: Replace '...having a role...' with '...responsible for...'. Training for recovery plans and incident response is fundamentally different than the general cyber security training and should not be rolled into a 'one size fits all' training requirement.More clarity is needed on identity verification, how often does it need to be checked, does a copy need to be retained.
12.78	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
12.79	We Energies	Disagree	We Energies agrees with EEI suggestion: R2 contains two very subjective words: "sound" and "essential." Suggest striking these words.
12.80	GTC & GSOC	Disagree	We recommend removing the word "all" in R2 to ensure that you do not have to track

#	Organization	Yes or No	Question 12 Comment
			and document reinforcement for each and every individual. We also recommend that R3.2 “For personnel having specified electronic access to any BES Cyber System” be clarified to identify to what “specified” access this is intended to apply.We recommend R2 through R4 should distinguish between the different types of users and administrators that have different responsibilities and access and therefore need different levels of training.R4 needs to be revised to better reflect the limitations of performing background checks on persons who have resided even briefly in foreign countries.
12.81	Xcel Energy	Disagree	We think R2 should be clarified to note that wide-distribution information such as company newsletters or e-mails satisfy the quarterly reinforcement requirement and that tracking on an individual basis is not required.
12.82	MRO's NERC Standards Review Subcommittee	Disagree	We would propose replacing the terms “provide all” with “make available to all”, as we are concerned the word “provide” could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were “provided” to each individual employee.
12.83	The Empire District Electric Company	Disagree	We would propose replacing the terms “provide all” with “make available to all”, as we are concerned the word “provide” could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were “provided” to each individual employee.
12.84	Entergy	Disagree	Wording in R2 is very awkward. Language needs to be written more concisely to show that awareness modules simply need to be disseminated. Current language allows for misinterpretation. It could be assumed that evidence to prove that modules have not only been disseminated but have also been received by appropriate personnel is required. The language incorporated into R3 for emergency provisions is similar to that found in CIP-003-3, R1.1, but seems to be restrictive to only cyber security training and personnel risk assessments in R4. These emergency provisions (which should be approved by the Senior Manager or Delegate) should continue to be allowed for all

#	Organization	Yes or No	Question 12 Comment
			standards/requirements, if a potential impact to emergency response or the BES subsists. Efforts to add newly created topics to the cyber security training module should be minimal. R3.5 adds clarity by replacing the word "annual" with "every 12 months". CIP-011, R4 is largely unchanged from CIP-004-3, R3. Criteria for an acceptable personnel risk assessment appears to be more lenient and allows for identity verification via a government-issued photo ID, as opposed to the social security check that was required for v3. Language is a little unclear as to which types of government-issued IDs are permissible. Are government-issued IDs from different countries (Mexico, Iran, etc.) acceptable? Additional specificity is needed.
12.85	Verizon Business	Agree	For section 3.1, "Escort Management:" should be a required item for the Cyber Security Training. In paragraph R4, the first sentence should be revised to read as follows (bolded is added text): "Each Responsible Entity shall ensure a personal risk assessment is performed and reviewed and approved by the Responsible Entity for all personnel…." 4.1, First Bullet – This could refer to the requirements of U.S. Form "I-9" for verification to work in the U.S. By passing the requirements of I-9, one satisfies this CIP-011 requirement. In paragraph 4.2, the requirement should be amended to read (bold is added text): "Each Responsible Entity shall document the results of each personnel risk assessment and they shall document that the results were reviewed and accepted or rejected as an acceptable risk for the Responsible Entity.

13. Do you agree with the proposed definitions for external connectivity, routable protocol, and non-routable protocol? Please explain and provide any suggestions for modification.

Summary Consideration:

While some commenters indicated support for local definitions, most commenters suggested moving the definitions to the NERC Glossary instead. In response, the SDT has moved all definitions to the NERC Glossary and discontinued the use of local definitions.

Several commenters expressed the need to bring back the concept of an Electronic Security Perimeter, because otherwise, the definition of "external connectivity" makes it difficult to determine at what point in the communication path a device is external. The SDT generally agrees with these comments and has reintroduced the definition of an "Electronic Security Perimeter" as a collection of Electronic Access Points.

Several commenters made suggestions about the use of the term "routable." The suggestions provided include more examples of routable versus non-routable protocols and the use of the OSI seven-layer network model. Others noted the term "routable external connectivity" is used, but "routable protocol" is never used. In response, the SDT has only defined the term "**External Routable Connectivity**" as follows: *"The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol."*

Commenters expressed confusion about the term BES Cyber System and requested additional guidance. In response, the SDT has added considerably more detail about the Reliability Operating Services a BES Cyber System performs along with the types of assets considered as part of the BES Cyber System.

#	Organization	Yes or No	Question 13 Comment
13.1	WECC		This should be defined at the top of the standard, dislike the definition box in the middle of a requirement.The use of external connectivity and/or enabled routable protocols to differentiate between required and non-required controls should be reconsidered. In most cases, the controls are still necessary to protect against insider threats.
13.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.

#	Organization	Yes or No	Question 13 Comment
13.3	ReliabilityFirst Staff	Agree	Does the drafting team intend to include these terms in the NERC Glossary of Terms?
13.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	However, this does not come up until well into the Standard. It is not clear how programmable electronic devises having no external connectivity, routable protocol, or non-routable protocol are treated. How shall programmable devises be treated when the only connectivity is on site connection to a laptop computer?
13.5	Puget Sound Energy	Agree	Puget Sound Energy would like to note that, with the widespread use of Internet Protocol (IP) as the communication protocol for the majority of Cyber Systems on the planet, if the standard is trying to be more inclusive of routable protocols than just IP, it should give some examples of others. "Routable Protocols" is an extremely technical concept, when talking about routable protocols other than IP, which could greatly impact scope, reliability, response, and overall compliance. If the standard is being specific to IP, then it should clarify that. If the standard is referencing other routable protocols than IP, then it should give some examples. (Ex: Routable protocols include, but are not limited to, IP, DecNet, MPLS, etc...).
13.6	Kansas City Power & Light	Agree	Recommend moving these definitions with R6 where routable protocol is first referenced.
13.7	Emerson Process Management	Agree	The current draft standard does away with the perimeter concept. It becomes slightly difficult in defining "internal" and "external."
13.8	LCEC	Agree	The definitions sound good but I do not agree with the use of "Required for external connectivity only" within the tables as they do not make sense most of the time.
13.9	SCE&G	Agree	The proposed definintions should be added to the "definitions table" at the front of the standard, rather than just in the boxes throughout the standard.
13.10	Allegheny Power	Agree	The proposed definitions are helpful, and should be used more extensively within the requirements to identify controls that are appropriate to devices based upon their

#	Organization	Yes or No	Question 13 Comment
			functionality/vulnerability.
13.11	EEI	Agree	The proposed definitions are helpful, and should be used more extensively within the requirements to identify controls that are appropriate to devices based upon their functionality/vulnerability.Suggested modification for R3:"Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access except for emergency circumstances that are approved by the senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response."Suggest elimination of Table R3.Suggested modification for Requirement 3.2:"For personnel that have a role in maintaining networking hardware and software supporting a BES Cyber System, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems" In general, the drafting team needs to account for a person's "need to know" within the training program.
13.12	Florida Municipal Power Agency	Agree	These definitions ought to be associated with the first requirement that uses the definitions. As it appears now, these definitions seem associated with R3 on training, which has nothing to do with these definitions.
13.13	Electricity Consumers Resource Council (ELCON)	Agree	We agree with the definitions but they should be applied to limit the applicability of all the requirements in the standard.
13.14	Cogeneration Association of California and Energy Producers & Users Coalition	Agree	We agree with the definitions; however, they should be applied to limit the applicability of all of the requirements in the standard.
13.15	We Energies	Agree	We Energies agrees with EEI comment: The proposed definitions are helpful, and should

#	Organization	Yes or No	Question 13 Comment
			be used more extensively within the requirements to identify controls that are appropriate to devices based upon their functionality/vulnerability.We Energies agrees with EEI: Suggested modification for R3:Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access except for emergency circumstances that are approved by the senior management official identified in Requirement R1 or their delegate and impact the reliability of the BES or emergency response.We Energies agrees with EEI: Suggest elimination of Table R3.Suggested modification for Requirement 3.2:For personnel having electronic access to any BES Cyber System, this cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.
13.16	FirstEnergy Corporation	Agree	While in agreement with the definition of routable protocol, it does not provide enough clarity. Would like to see the definition expanded to include protocol encapsulation.
13.17	US Bureau of Reclamation	Agree	Yes, but the definitions appear in the wrong location within the Standard.
13.18	Independent Electricity System Operator	Disagree	- External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?
13.19	Consultant	Disagree	1. Suggest deleting the words "for the purpose of this standard". These words are unnecessary and obfuscate the term being defined. Once the standard is approved these terms should be added to the NERC glossary as part of the next update process for that document.2. The term being defined should be capitalized, as it is now a defined term.3. Suggest listing these definitions in a section of the standard, and deleting these text boxes. Locating them in these text boxes makes the requirements difficult to read.4. If the definitions have to be injected like this, it is not clear why these definitions are located here. Nothing in these requirements discusses the terms being defined.5.

#	Organization	Yes or No	Question 13 Comment
			Suggest deleting "is defined as" as unnecessary. Suggest the format below:External Connectivity - Data communication across the protected electronic boundary. (Addressed in R20.) This definition also relates to the definition of Electronic Access Point in R20.Routable Protocol - a communications protocol that contains a network address as well as a device address thereby allowing packets to be forwarded from a device on one network to a device on another network. Non-Routable Protocol - a communications protocol that contains only a device address and not a network address that not incorporate an addressing scheme for sending data from a device on one network to a device on another network.
13.20	NextEra Energy Corporate Compliance	Disagree	Although on the surface these definitions are straight forward, NextEra believes there is a need to make a transition from the previous requirements for access points. There is not a strong tie between the definition for external connectivity (routable or not) to the requirements in the following sections. For example, Is a serial connection to a BES Cyber considered an Access Point to be protected? The definitions and requirements for protection need to be consistently applied across different levels of impact.
13.21	Garland Power and Light	Disagree	Comment - TOP definition needs to reword as follows:For the purpose of this standard, external connectivity is defined as a data communication path from a BES Cyber System Component to a device external to the BES Cyber System.Suggest better routable and non-routable protocols definitions - give examples of routable and non-routable protocols ie. tcp/ip, netbios, ipx, appletalk,
13.22	Network & Security Technologies Inc	Disagree	Current proposed definition of “external connectivity” is basically circular and could be interpreted in a number of ways. As written, it could even be applied to situations where two discrete BES Cyber Systems are connected to the same LAN segment, which we assume is not what the SDT intended. Suggestion: Unless the SDT really does intend for any network connection not entirely “within” a BES Cyber System to be considered “external,” rewrite the definition to provide a better point of reference than the BES Cyber System itself. Towards that end, the SDT might reconsider its decision to scrap the term, “Electronic Security Perimeter” (which, we note, still appears in CIP-011 in the

#	Organization	Yes or No	Question 13 Comment
			language of R20). We believe that in the context of current CIP Standard CIP-005, "external" connections are widely understood to be defined relative to the logical boundary of an ESP.
13.23	US Army Corps of Engineers, Omaha Distirc	Disagree	Definition of external connectivity is loose and problematic in the interplay with the loose definition of BES Cyber System. Does a communication path exist through a firewall? Does the term mean only intended paths?
13.24	Dominion Resources Services, Inc.	Disagree	Dominion has concerns about the definitions of external connection and electronic access point (Boundary Protection) as illustrated in the following example:A power station has 3 units with the same control system and a shared process I/O bus. Each unit has a control room with MMI, a dedicated server that is networked to the servers at the other 2 units, a front-end processor that is networked to multiple PLCs which are connected to smart I/O controllers. The servers are connected through a firewall to the central engineering office.Under this scenario, it is unclear where the BES Cyber System boundaries should be drawn. If the boundary is drawn around the station, everything is likely to be classified as High Impact and hundreds of I/O transmitters would be included that would normally be Low Impact. If an attempt is made to break the BES Cyber Systems down by unit, every interconnection between the units becomes an external connection and an electronic access point. Excluding a PLC from being part of the High Impact system is difficult because the PLC becomes the electronic access point and its data becomes an external connection. Boundary Protections with the PLC or its connection to the data bus cannot be met.The definition of a "communications path" needs to be clarified. Dominion proposes the following alternate wording to clarify the intent of the definition for external connectivity: ".....external connectivity is defined as any digital communication with a BES Cyber System component from a source external to the BES Cyber System."
13.25	E.ON U.S.	Disagree	E.ON U.S. believes that external connectivity should specify that it is going through an "access point" per the current definition of an access point. The definition of "external connectivity" references the existence of a "data communications path." Does this take

#	Organization	Yes or No	Question 13 Comment
			into consideration any protective measures that assist in the isolation or blocking of data communications? For instance, if a BES Cyber System or Component has a network connection, even an indirect one with multiple levels of firewalls and other security protective devices, to another "external" devices, does it have external connectivity? If so, virtually every system is externally connected; only those that are completely electronically/network-isolated would not be
13.26	USACE - Omaha Anchor	Disagree	External connectivity definition is incorrect. Would prefer a definition external to the facility or external to the electronic security perimeter (understanding that term doesn't exist in this standard.)
13.27	Black Hills Corporation	Disagree	External Connectivity is too open to interpretation; needs to distinguish between external and remote connectivity.
13.28	Luminant	Disagree	External connectivity should include any path and not just those that are considered part of the system functionality. Should also only include routable connectivity
13.29	Progress Energy (non-Nuclear)	Disagree	How are these terms applicable? Is this the key that will take many of our microprocessor relays in Transmission out of scope? If so, we need a clearer linkage to the definitions. It is still not clear if a non-routable protocol like VanCom is definitely excluded. If VanCom is not excluded as it was with previous standards, then every transmission RTU is pulled into consideration.Why have these definitions if the programmable electronic device definition is in play? Again is NERC's intent to manage at component, subsystem, or plant system level? Seems like impact would vary depending to what level of detail we need to get to.These terms are used very limited in CIP 11 and when used they are not used as individual terms. They are combined ie. "external routable connectivity".Do we have to use "routable protocols" term versus the ISO model...like layer 3 and greater?
13.30	Turlock Irrigation District	Disagree	In the definition of external connectivity the use of the words "data communications path" are confusing. Perhaps external connectivity could be defined as "Any electronic

#	Organization	Yes or No	Question 13 Comment
			access point that allows data to be transmitted and/or received between a defined BES Cyber System and a device that is not part of the defined BES Cyber System".
13.31	Southwest Power Pool Regional Entity	Disagree	It is unclear whether the definition of routable protocol includes Layer 2 devices in its scope, understanding that entities have had a difficult time distinguishing between a communications protocol and the networking infrastructure supporting the protocol's use. Additionally, given that the standard is now identifying BES Cyber Systems based upon the reliability functions they perform or support, is it even appropriate to continue to distinguish between routable and non-routable protocols? It is the function and the span of control of the Cyber Asset that determines the impact categorization and requirements applicability.
13.32	National Grid	Disagree	National Grid recommends changing from "from a device external to the BES Cyber System" to "from a device external to the BES Cyber System Boundary"
13.33	LADWP	Disagree	Needs brighter lines.
13.34	ISO New England Inc	Disagree	needs work - removable of ESP has implications. Needs better definition, use of routable protocol clouds issue. External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?Recommend changing from "from a device external to the BES Cyber System " to "from a device external to the BES Cyber System Boundary"
13.35	Dairyland Power Cooperative	Disagree	Once the identification of external connectivity is made, why is it relevant to distinguish routable vs. non-routable? A serial cable connected to an unprotected facility may be much more risky than a routable protocol with strict limitations on routing. There may be distinctions to be made in system or communication related requirements, but for training, the external connectivity criteria alone would be the best criteria for the impact level distinctions.

#	Organization	Yes or No	Question 13 Comment
13.36	Public Service Enterprise Group companies	Disagree	Please define the meaning of “routable external connectivity”. The terms “external connectivity”, “routable protocol”, and “non-routable protocol” were defined but not “routable external connectivity” is not. In particular, please clarify the language to provide that if an IP based protocol is in use for a BES Cyber System (e.g. at a substation) where the network address is not required and there is no “external connectivity” (i.e. the IP routing capabilities are disabled - there are no routers or devices capable of routing an IP datagram), this would result in the BES Cyber System being categorized as not having “routable external connectivity”.
13.37	Hydro One	Disagree	Recommend changing from “from a device external to the BES Cyber System” to “from a device external to the BES Cyber System Boundary”.
13.38	Northeast Power Coordinating Council	Disagree	Recommend changing from “from a device external to the BES Cyber System” to “from a device external to the BES Cyber System Boundary”.
13.39	Con Edison of New York	Disagree	Routable Protocol is defined as a communications protocol that contains a single address which identifies both the network and a unique device on that network.
13.40	San Diego Gas and Electric Co.	Disagree	SDG&E recommends rewording and clarifying the definitions of an External and Internal BES Cyber System and Remote Access. Connectivity is defined as “a data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System.” 1) What are the standard elements, configuration items, or technology implementations which would distinguish an internal and external BES Cyber System? For example, using this definition, Cyber System A could be on the same LAN as Cyber System B, but considered “external” because the “data communication path” exists (and is switched and not routed) between the 2 Cyber Systems, and 3) does a “data communication path” include serial, USB, Wireless, Channel Attached, or other data communication types of transport? We feel that the access concepts and Remote Access definitions are unclear and difficult to decipher.

#	Organization	Yes or No	Question 13 Comment
13.41	Northeast Utilities	Disagree	Suggest revising the local definition for external connectivity to add “boundary” so the definition would read “... from a device external to the BES Cyber System Boundary”.
13.42	Allegheny Energy Supply	Disagree	Suggest that the External Access definition be revised to include the concept that external access is communcations path access outside of the electronic and physical protection boundaries of BES Cyber System or its connected networks.
13.43	Duke Energy	Disagree	Suggest using these definitions in CIP-010. For generation stations in particular, external connectivity and remote connectivity (R11) should be defined as remote/external to the protected network rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome with little value to cyber security. Same for R13.
13.44	Alberta Electric System Operator	Disagree	The AESO would like to see the terms “network address” and “device address” further defined, to limit possible ambiguity. Consider taking frames (e.g. Ethernet or 802.3) into account in the definition, in addition to packets.
13.45	Southern Company	Disagree	The definition of external connectivity should make it clear that a data communication path does not include human action as an intermediate step.
13.46	Matrikon Inc.	Disagree	The definition of routable protocol should be congruent with the OSI networking stack <http://en.wikipedia.org/wiki/OSI_model>. Routable protocols are those which provide capabilities to communicate at OSI "Network" Layer 3.External connectivity definition still has room for interpretation. If we continue the approach of following the OSI model, then external connectivity is: a communication data "session" using a routable protocol, to an external network requiring OSI Layer 3 "router" or "access point"in order to communicate to an extended network.

#	Organization	Yes or No	Question 13 Comment
13.47	Entergy	Disagree	The definitions for routable and non-routable protocol appear to be satisfactory. However, the definition of external connectivity could prove troublesome, depending upon one's interpretation of a BES Cyber System. For example, a backup site may be classified as a different BES Cyber System than that of a primary site, thus making each one external from the other. Utilizing this interpretation could cause complications from an external connectivity perspective. Conversely, if both sites were classified as a single BES Cyber System, then the issue for external connectivity would not exist.
13.48	US Army Corps of Engineers	Disagree	The proposed definition states that external connectivity is defined as a data communication path existing to a BES Cyber System Component from a device external to the BES Cyber System. Does the use of the word "existing" mean that the data communication path is permanent? If a plant allowed dial-up connectivity to their BES Cyber System, but would need to physically connect the modem for the outside person to dial-in everytime, and then disconnect the modem when completed, leaving an air-gap, would that count as "external connectivity" in this definition?
13.49	Indeck Energy Services, Inc	Disagree	The term “routable protocol” is used only once and the term “non-routable protocol” is never used except in the definition. “Routable connectivity” or “routable external connectivity” are used multiple times without definition.
13.50	Nuclear Energy Institute	Disagree	These definitions should appear in the “Definitions” section.Additionally, for generation stations in particular, external connectivity and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome with little value to cyber security. Same for R13.
13.51	MidAmerican Energy Company	Disagree	This definition depends on the definition of a BES Cyber System Component, deferring to the functionality of the connected device as the differentiating factor between internal

#	Organization	Yes or No	Question 13 Comment
			and external connectivity. By this definition, a device providing "control" of the BES is by definition a "BES Cyber System Component" and thus, is NOT qualified as external connectivity. For example, a personal home PC, using an Internet connection, could provide "control" of the BES, and thus be considered a BES Cyber System Component, and thus by definition, is not considered remote access.We propose that the definition of external connectivity somehow incorporate the concept of communication medium and endpoint/host control. If the entity does not have 'control' of the medium over which the communications occur, then the communication path must be deemed 'external connectivity'. Additionally, if the entity does not have 'control' over the endpoints/hosts on both ends of the communications path, then the communication path must also be deemed 'external connectivity'. In short, any communication path to a BES Cyber System Component for which the entity does not "control" the communication medium or does not have "control" over both communication endpoints and devices communicating through the endpoints, should be considered 'external connectivity'.Of course, the key consideration in this definition is what constitutes 'control'. The CIP standard for physical security perimeter protections for hosts and endpoints is a good place to start, with the understanding that logical controls such as encryption are viable alternatives for communication paths.If the definition of external connectivity is intended to include dial-up connectivity it should be expressly stated.
13.52	PacifiCorp	Disagree	This definition depends on the definition of a BES Cyber System Component, deferring to the functionality of the connected device as the differentiating factor between internal and external connectivity. By this definition, a device providing "control" of the BES is by definition a "BES Cyber System Component" and thus, is NOT qualified as external connectivity. For example, a personal home PC, using an Internet connection, could provide "control" of the BES, and thus be considered a BES Cyber System Component, and thus by definition, is not considered remote access.We propose that the definition of external connectivity somehow incorporate the concept of communication medium and endpoint/host control. If the entity does not have 'control' of the medium over which the communications occur, then the communication path must be deemed 'external connectivity'. Additionally, if the entity does not have 'control' over the

#	Organization	Yes or No	Question 13 Comment
			endpoints/hosts on both ends of the communications path, then the communication path must also be deemed 'external connectivity'. In short, any communication path to a BES Cyber System Component for which the entity does not "control" the communication medium or does not have "control" over both communication endpoints and devices communicating through the endpoints, should be considered 'external connectivity'.Of course, the key consideration in this definition is what constitutes 'control'. The CIP standard for physical security perimeter protections for hosts and endpoints is a good place to start, with the understanding that logical controls such as encryption are viable alternatives for communication paths.If the definition of external connectivity is intended to include dial-up connectivity it should be expressly stated.
13.53	GTC & GSOC	Disagree	We recommend that local definitions for a specific Reliability Standard be documented in a section prior to the requirements sections instead of interspersed throughout the requirements. While it may improve the initial readability of the requirements, it is problematic in the long term determining if and where a particular word is defined.We also recommend "external connectivity" should be limited to situations where an external device can initiate a connection to the BES System Component. If a firewall limits connections to only those initiated by the BES System Component itself (i.e., connections are only one-way: out), the component should not be considered to have external connectivity.We recommend deleting the portion referring to network and device addresses because not all protocols make a clear distinction between a network address and a device address. The functional packet-related distinction is sufficient. The second and third paragraphs of the definition would read: "For the purpose of this standard, a routable protocol is defined as a communications protocol that allows packets to be forwarded from one network to another.For the purpose of this standard, non-routable protocol is defined as a communications protocol that does not incorporate an addressing scheme for sending data from one network to another."
13.54	Bonneville Power Administration	Disagree	We understand the need to keep definitions close to where they're used, it is also important to have them centrally located. We understand that this leads to a document maintenance issue. However, most document creation tools have solutions. For

#	Organization	Yes or No	Question 13 Comment
			instance, in Microsoft Wordâ„¢, you can make the definition a bookmark, and then insert a cross-reference somewhere else. The definition of "External Connectivity" is too broad. Consider an example: A user in a Control Center is logged into a workstation that is part of a BES Cyber System. The user opens a connection from that workstation to another BES Cyber System in the same Control Center. The communications path is totally under the control of the Responsible Entity, and all systems and communication paths involved are under the physical and electronic protections of the Control Center. Yet, this would constitute and external connection to the second BES Cyber System, and thus constitute remote access to that system. This is an untenable situation, especially considering the tight controls justifiably required for connections from outside the control of the Responsible Entity.Recommendation: "...defined as a data communications path to a BES Cyber System that encompasses, in some or all portions, links outside the control of the Responsible Entity." The definition of "Routable Protocol" is acceptable.The definition of "Non-routable Protocol" is slightly broader than necessary. It excludes point-to-point protocols. For instance, RS232 is one of many serial communications protocols that contains no address of any kind. Recommend changing "...that contains only a device address and not a network address." to "...that contains at most a device address and no network address."
13.55	Verizon Business	Disagree	1) The definition should explicitly state that a “Routable Protocol” includes TCP/IP. Also, the definition should explicitly state that MPLS is considered a “Routable Protocol” because MPLS is considered OSI Layer “2 ½” and hence there may be disagreement whether it is routable. For a “Non-Routable Protocol,” an example like a protocol in the OSI Layer 2 should be provided. 2) The term “external connectivity” requires more explanation. It is unclear whether it would include two BES Cyber Components that are connected to each other, regardless of the length of separation.

14. Tables R3 and R4 provide direction concerning what impact level of BES Cyber Systems to which Requirements R3 and R4 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R3 and R4 have moved to CIP-004-5 R1 through R3.

Several commenters expressed confusion regarding the purpose of specifying routable connectivity in the applicability for training requirements. The SDT agrees and has modified the applicability to include all High and Medium BES Cyber Systems.

In addition, several commenters suggested the training and personnel risk assessment should apply across all impact levels. One commenter suggested the training and personnel risk assessment should only apply to the High Impact level of BES Cyber Systems, and another commenter suggested there should also be a "no-impact" level. The SDT has changed the requirements for training and personnel risk assessments to apply to High and Medium Impact BES Cyber Systems. These requirements do not apply to Low Impact BES Cyber Systems because of the significant effort required to track the Low Impact BES Cyber Systems and the persons who have authorization to access those systems.

#	Organization	Yes or No	Question 14 Comment
14.1	US Army Corps of Engineers		In Tables R3 and R4, the phrase "Physical access to BES Cyber Systems" is qualified with the words "with routable external connectivity" but these words are not referenced in any of the paragraphs R2-R4. Paragraphs R2-R4 state physical access as "authorized unescorted physical access to BES Cyber Systems." Should we assume that both terms are the same?
14.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
14.3	Northeast Utilities	Agree	Please change Table R4 to read "Personnel Risk Assessment".
14.4	Madison Gas and Electric Company	Agree	Thank you for adding these helpful tables immediately after the requirement. This reduces the confusion of turning a page to an appendix.

#	Organization	Yes or No	Question 14 Comment
14.5	GTC & GSOC	Agree	We recommend making sure there is consistency with impact levels for authorizing physical and authorizing electronic access
14.6	Black Hills Corporation	Agree	Would like to know if an entity exceeded any NERC requirements as internal policy, and subsequently had an individual miss training who did not interact with a BES Cyber System, would this be considered a violation by NERC.
14.7	ERCOT ISO	Disagree	3.2 & 4.2: Please clarify why "with routable external connectivity" is addressed.
14.8	US Army Corps of Engineers, Omaha Distirc	Disagree	3.2 not clear as to purpose of this training or how external connectivity relates. Without electronic access the most they could do is damage hardware. Does this only apply to hardware providing external connectivity such as firewall etc?
14.9	Tenaska	Disagree	5.3 Consider leaving the word "uniquely" out or change it to say individually identify.
14.10	BCTC	Disagree	Â We are in strong disagreement with R3.2. We have various parties who have electronic access to our BES Cyber Systems but do not agree that training these individuals on networking hardware and connectivity would increase the security of the BES. Could you please clarify the objective of this requirement? - i.e. why would someone who simply accesses a console to view BES Cyber System data require network-related training? We recommend that the requirement be worded something like "... personnel will be supplied training on applicable NERC CIP devices that they are authorized to work on and the associated related security controls, as identified in the CIP Standards..." Above we have recommended above that "emergency situation" language remain at the security policy level. A potential scenario in this requirement is an emergency occurs (i.e. a critical piece of equipment breaks) whereby the closest service provider available to fix the problem is minutes away but has not completed CIP training or a PRA; from an operations (i.e. "keeping the lights on") perspective we would identify this as an emergency situation, seek approval from our Senior Manager or delegate to allow this person to access our facility, and allow the repair to occur. In this scenario we are assuming our 'regular' service technicians are unavailable or far way

#	Organization	Yes or No	Question 14 Comment
			from the facility.Â We have encountered an issue where some non-North American countries will not disclose criminal histories so it will be difficult to meet the requirement that states ... “A seven year criminal history records check covering all locations where, during the previous seven years up to the current time, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration.” We can have new employees from these countries start employment but lived in North America for less than 7 years. For such a scenario we recommend that the language be revised to indicate that the Utility requests a seven year criminal history check on a best efforts basis; i.e. we can ask for the information but there is no guarantee the originating country will provide us with the results - this is beyond our control. FYI, simply denying a person on these grounds in Canada violates out employment legislation.Â R4.2 We currently retain a “clear”/ “not clear” result with all PRAs for contractors and employees. Please confirm that this requirement does not require the Utility to retain detailed records (i.e. listing of criminal offenses, charges, etc.)
14.11	Hydro One	Disagree	Agree provided the external connectivity definition is revised per the response to question 13.Recommend changing Table R4 from “personal” to “personnel”.Suggest changing to annually for consistency.Such classification will add additional unnecessary burden since specific training will need to be generated and tracked depending on the type of system access
14.12	Northeast Power Coordinating Council	Disagree	Agree provided the external connectivity definition is revised per the response to question 13.Recommend changing Table R4 from “personal” to “personnel”.Clarify “12 months”.
14.13	ISO New England Inc	Disagree	Agree provided the external connectivity definition is updated per answer #13 Table 4 title uses “personal” instead of personnel.
14.14	San Diego Gas and Electric	Disagree	Attempting to split hairs between PRA and Training requirements for physical and cyber access to BES Cyber Systems for Medium and High Impact systems seems to

#	Organization	Yes or No	Question 14 Comment
	Co.		unnecessarily increase risk exposure for an Entity and complicates the process and controls needed to meet R3 and 4 of CIP-011-1. SDG&E recommends that the requirements for both of these tables be required for High Impact BES Cyber Systems only
14.15	E.ON U.S.	Disagree	CIP-011, R3 states that contractors and service vendors with authorized electronic or unescorted physical access are to complete cyber security training before given this access. However, this begs the question of what constitutes satisfactory evidence of this training for these individuals? If vendor-provided training is adequate, what evidence is needed to maintain this training?a. (3.2) "...shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity..." For most users of these systems, training on the networking hardware and software provides little or no value. Unless these are systems administrators tasked with responsibilities for managing / monitoring these systems, users (and associated training) should be focused on the functions of the system to support operation, monitoring, and control for which they are responsible.CIP-011, R4 requires background checks for contractors and service vendors. The new requirements do not clarify the acceptable evidence required to be maintained by entities. Is it acceptable for a service provider to conduct the background checks? If so, what evidence of background checks does the registered entity need to maintain?Does the requirement apply for everyone that has access to the BES cyber system ? Would this include support personnel and janitorial staff? E.ON U.S. suggests that the requirement be tied to job function rather than a blanket requirement for all.E.ON U.S. requests clarification as to how personnel that only have remote access to the system should be verified. Photo IDs are neither practical nor required.
14.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
14.17	US Bureau of Reclamation	Disagree	Cyber access training and personnel risk assessment requirements should be applied to

#	Organization	Yes or No	Question 14 Comment
			all three impact levels.
14.18	BGE	Disagree	Define “electronic access” as noted in table R3 (3.1). 3.2 Should say “Physical access to BES Cyber Systems (remove routable external connectivity). Table R4 (4.2) should add “unescorted” physical access to BES.....
14.19	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes Personnel Training, Awareness, and Risk Assessment should only apply to personnel with access to high impact BES cyber systems and not include personnel with access to medium and low impact systems. This requirement as currently drafted is unduly burdensome for field personnel that have local access to programmable electronic devices. These personnel need not be aware of network considerations to securely perform their job duties.
14.20	Luminant	Disagree	Does R4, 4.1 need to be modified to address valid identification for foreign nationals with remote (overseas) access to BES Cyber Systems?
14.21	MRO's NERC Standards Review Subcommittee	Disagree	For item 3.1 and 3.2, we propose making the Low Impact criteria “Required”. Cyber Security Training is something that should probably be carried out across the BES.For item 3.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.For item 4.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.If an entity is required to restrict physical access, then they should also be required to provide training.
14.22	The Empire District Electric Company	Disagree	For item 3.1 and 3.2, we propose making the Low Impact criteria “Required”. Cyber Security Training is something that should probably be carried out across the BES.For item 3.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external connectivity only”.For item 4.2, we would propose removing “with routable external connectivity”, and then adding the following under Medium Impact:”Required for routable external

#	Organization	Yes or No	Question 14 Comment
			connectivity only".If an entity is required to restrict physical access, then they should also be required to provide training.
14.23	Platte River Power Authority	Disagree	Is the intent that prior training is not required for Physical access to BES Cyber Systems without routable external connectivity? In other words, the table says that prior training is only required if Physical access is granted to a BES Cyber Systems with external connectivity. Is that the intent?
14.24	Entergy	Disagree	It appears nonsensical to require cyber security training and personnel risk assessments for electronic access to BES Cyber Systems classified as Medium-impact, but not for physical access to Systems with external connectivity. Requiring these items for only one type of access and not the other merely increases the likelihood of misinterpretation of the requirements by the Entity. PRAs and training should be required for both types of access or neither.
14.25	FirstEnergy Corporation	Disagree	It would be very difficult to administer training and PRAs based on impact levels. It seems like it would be easier to just have one level for all. We suggest eliminating the tables/impact levels for R3 and R4.Training and PRAs should be required for all levels. It is easier to maintain, track and move employees around if they are all trained and background checked, especially with the need to continuously reassign employees.
14.26	Manitoba Hydro	Disagree	Manitoba Hydro agrees that cyber security training is not a standard requirement for all personnel who have unauthorized physical access to Low Impact BES Cyber Systems, and therefore should not be auditable. We do not agree that training is not a requirement for personnel who have authorized electronic access to Low Impact BES Cyber Systems, and suggest that it be an auditable requirement.
14.27	Progress Energy (non-Nuclear)	Disagree	May not be an issue since most our personnel that require access will very likely require access to all three impact levels and will require adherence to the highest security level anyway. It does not seem practical and reasonable to develop and maintain three different security programs based on the three impact levels.The question with most of

#	Organization	Yes or No	Question 14 Comment
			the impact level requirements is the difficulty and cost associated with developing and maintaining three different levels of security, monitoring and controls and making sure that the appropriate levels are applied with an increase in impact level.Again is NERC's intent to manage at component, subsystem, or plant system level? Impact will vary depending to what level of granularity we need to get to.Section R3.1 appropriately provides for a level of NERC CIP training consistent with physical only access. The last point 'Identification and reporting of a Cyber Security Incident' should be clarified to be the physical aspects of a cyber security incident. Since this is the type of training that we will be providing to janitors/HVAC repair technicians/electricians, there should not be a requirement to provide any type of cyber training. The full 'Identification and reporting of a Cyber Security Incident' can be included under R3.2 - which is intended for those with actual cyber access.
14.28	National Grid	Disagree	National Grid agrees provided the external connectivity definition is updated per answer 13.Recommend changing Table R4 from "personal" to "personnel".
14.29	LCEC	Disagree	No. These tables should include all standards and clearly indicate their intent.
14.30	American Municipal Power	Disagree	Please add a little or no impact category.
14.31	Puget Sound Energy	Disagree	Puget Sound Energy, as stated earlier in this document, would need to see more specific definition to "Low", "Medium", and "High" impact, as well more specific definition to subjective terms such as "restrict" and "affect". If specificity can be provided to the subjective areas of the definition to "Low Impact", "Medium Impact", "High Impact", "restrict control", and "affect situational awareness", Puget Sound Energy agrees with the tables.
14.32	ReliabilityFirst Staff	Disagree	Requirement R4.1; ReliabilityFirst is concerned that permitting documents other than Social Security Identification for identity verification could lead to questionable results. Requirement R4.3 only addresses updating a PRA every seven years but does not include

#	Organization	Yes or No	Question 14 Comment
			a requirement to update the PRA "for cause." Table R3 and R4, Medium Impact BES Cyber Systems should be required for rows 3.2 and 4.2 respectively.
14.33	Southwest Power Pool Regional Entity	Disagree	Some degree of physical and electronic access training is basic security training that should be applicable to all impact categories. The extent of the training could perhaps be adjusted to reflect the impact categorization. 4.2: See the discussion regarding the need for distinguishing between routable and non-routable protocols. The Personnel Risk Assessment should be required prior to access for at least High and Medium impact BES Cyber Systems, both physical and electronic, regardless of any communications protocol being used.
14.34	Network & Security Technologies Inc	Disagree	Suggest (1) dropping "routable external connectivity" qualifier for High Impact systems in 3.2 and 4.2 and adding Medium Impact systems to 3.2 and 4.2.
14.35	EEI	Disagree	Suggest elimination of Table R3. EEI suggests making training mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.Suggest elimination of Table R4. EEI suggests making personnel risk assessment mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site?
14.36	Emerson Process Management	Disagree	Table R3 implies that Cyber Security Training is not required for people who have physical access to a high impact BES Cyber System as long as this system does not have routable external connectivity.Per 3.1, the training shall cover the policies, access controls and procedures.This is unclear about the connection between the needed training and the lack of routable external connectivity.Same note applies to Tabe R4.
14.37	American Electric Power	Disagree	Table R3, 3.2: Regarding "Physical access to BES Cyber Systems with routable external connectivity", suggested wording: "Authorized, unescorted physical access".Current

#	Organization	Yes or No	Question 14 Comment
			wording seems to require training for all physical access. Would a group taking a walking tour of a generation control room, transmission substation, or control center need cyber security training?Table R4, 4.2: Regarding "Physical access to BES Cyber Systems with routable external connectivity", suggested wording: "Authorized unescorted physical access"Current wording seems to require personnel risk assessment checks for all physical access. Would a group taking a walking tour of a generation control room, transmission substation, or control center need personnel risk assessments?
14.38	Alberta Electric System Operator	Disagree	The AESO suggests that security training and PRA are required for all impact levels for 3.1, 3.2, 4.1, 4.2 in the tables. The SDT should consider devising a graduated implementation scheme, or let the RE determine how much and to what extent the training and PRA should include for each impact level.
14.39	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS proposal to require cyber security training in Table 3.1 and Table 3.2 for all impact levels. The training requirements for Table 3.1 and Table 3.2 Low Impact, should only be required to comply with R3 sub-requirement 3.1, at a frequency of every 2 years. These Low impact facilities should not be required to comply with the specific requirements detailed in R3, sub-requirements 3.2-3.5. We suggest the table state; “Applies to sub-requirement 3.1 only, Frequency: Every 2 years” for Low Impact facilities. We agree with the MRO-NSRS comments on item 3.2; MRO-NSRS proposes removing “with routable external connectivity.”The APPA Task Force feels there is confusion with blanks in the tables. For example, in Table 4.1 we have assumed that a blank under the Low Impact category means a Low Impact BES cyber system is not required to conduct any Personal Risk Assessments Prior to Obtaining Table 4.1 and 4.2 access. If this is the meaning of such blanks it is our recommendation that the drafting team make that clear and insert a N/A for Not Applicable in all blanks throughout the document and define N/A in the introduction.For R4 Table 4.2, the APPA Task Force agrees with the MRO-NSRS proposal to remove “with routable external connectivity”, and to add the following under Medium Impact: “Required for routable external connectivity only”.The APPA Task Force suggests the following text for the noted tables:R3 Table 3.1: Low Impact: Required (Applies to sub-requirement 3.1 only) at

#	Organization	Yes or No	Question 14 Comment
			least once every 24 monthsMedium Impact: RequiredHigh Impact: RequiredR3 Table 3.2: Low Impact: Required (Applies to sub-requirement 3.1 only) at least once every 24 monthsMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR4 Table 4.1: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR4 Table 4.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required
14.40	Duke Energy	Disagree	The format in these tables is confusing. The requirements tell “what” the requirement is, and the table tells “who” the requirement applies to.
14.41	Con Edison of New York	Disagree	The R3 Dialog box defines external connectivity. It is not clear whether external activity is between systems in all cases, or does it mean between systems that are within different electronic boundaries. The wording needs to make this clear.The requirement to check photographic ID’s seem appropriate initially, or during the hiring process. As written it will require checking photo ID’s every seven years for an employee that has been working in for the Company for the entire period and whose identity should no longer be in question. The recurring requirement should not apply. R3.2 - it is unrealistic to expect to train operators on network equipment, software, and protocols, which is a separate and distinct job function.R3.3 - Review of DR procedures is appropriate, but specific training on DR is not
14.42	Consultant	Disagree	The 'required' blocks for electronic access would seem to imply that there is no connectivity between low impact assets and medium or high impact assets. If this is the case, then the table seems adequate. Or there should be a 'highest impact rules the network access controls' qualifying statement.The 'required' block for physical access would seem to imply that there is no co-located assets of different impact levels. This seems less likely than electronic access segregation. There should be a 'highest impact rules the physical boundary access controls' qualifying statement.
14.43	Idaho Power Company	Disagree	The table does not address training requirements for personnel with access to sensitive information about BES cyber systems but do not otherwise have electronic or physical

#	Organization	Yes or No	Question 14 Comment
			access to the system itself. It would be difficult to be compliant with R24 if personnel are not trained to recognize sensitive information or trained on the proper labeling and handling procedures.
14.44	Florida Municipal Power Agency	Disagree	The tables are ambiguous. For instance, is the blank in the table for R3 for Low Impact supposed to mean that no training is required, as FMPA interprets? FMPA believes that some level of training ought to be provided for all levels of impact, correlated with the impact level (e.g., biennially instead of annually for Low Impact for instance). FMPA suggests embedding the bullets into the table in a similar manner as R5 and leaving no blanks in the table to make clear what is required for each impact level.
14.45	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The tables should clearly specify unescorted physical access.
14.46	Constellation Energy Control and Dispatch, LLC	Disagree	-There should be a row in the R3/R4 tables for each Requirement/Sub-Requirement-Define "electronic access" in table R3 (3.1).-Table R4 (4.2) should say "unescorted" physical access to BES Cyber Systems with routable external connectivity.
14.47	Bonneville Power Administration	Disagree	Training and especially a PRA should be required for physical access to any High or Medium impact system, regardless of whether it has routable external connectivity. A hammer to a RAS system could cause severe issues, whether or not the system connects to field units with a routable protocol. In addition, physical access to BES Cyber Systems is potentially far more dangerous that Electronic Access (especially at field sites) The requirements in the table should be at least the same for physical and electronic access. In both Tables R3 and R4, the word “unescorted” should be added at the beginning of Items 3.2 and 4.2.
14.48	WECC	Disagree	Training should be done for all employees with any level of access to a minimum level. Additional criteria for training should be done dependent on the level of access and their

#	Organization	Yes or No	Question 14 Comment
			role. See previous comments about suggestion to replace with a requirement for a training and awareness program with specific criteria.These requirements should apply to all impact levels. Awareness, training, overall education, and personnel risk assessment are the building blocks for a successful security program.
14.49	We Energies	Disagree	We Energies agrees with EEI: Suggest elimination of Table R3. Make training mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.We Energies agrees with EEI: Suggest elimination of Table R4. Make personnel risk assessment mandatory for any personnel with authorized electronic access and/or authorized unescorted physical access to any BES Cyber Systems.We Energies agrees with EEI: Has the drafting team considered the challenge of performing photographic identification verification for personnel who may need authorized electronic access yet never come on site?
14.50	Minnesota Power	Disagree	While the impact levels seem reasonable, it is the inclusion of the term “external connectivity” as a qualifier in sections 3.2 and 4.2 of Tables 3 and 4 respectively that creates confusion. The relevance of connectivity to implementing appropriate physical security measures is not clear. Physical Access averts the need for electronic access, so this seems counterintuitive to include “external connectivity” as a provision. Minnesota Power recommends that sections 3.2 and 4.2 of Tables 3 and 4 respectively simply state “Physical access to BES Cyber Systems.”

15. Requirements R5 and R6 of draft CIP-011-1 concern procedures for physical security, which were previously contained in CIP-006. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Summary Consideration:

Many of the commenters expressed concerns with the timing of the revocation requirements as being unrealistic, especially for authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access. Commenters stated that the time required for revocation should be extended to 72 hours or to the next business day, whichever is longer, to allow for communications of this circumstance. Timing issues regarding the termination of access for contractors and/or service vendors were also raised.

The SDT has clarified that the timely revocation of electronic access to cyber systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform the assigned functions, that access should be revoked. Access is considered to be physical, logical, and remote permissions granted to all Cyber Assets comprising or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e.: physical access control system, remote access system, directory services). CIP-004-5 Requirement 7 enumerates the proposed requirements under a variety of conditions regarding revocation of access.

Some commenters expressed confusion regarding the use and meaning of the terms “grant” and “authorize” and their use in these requirements. Also, the term “Physical Access Control Systems” was requested to be defined, as the term will likely have different meanings for different entities and auditors and could lead to difficulties in implementation and auditing. The SDT has provided additional clarity in the requirements and has proposed the following definition for **Physical Access Control Systems**: *“Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers.”*

Physical security at remote substation sites was also raised as not being cost effective in preventing or detecting cyber attacks, especially for remote substations with only dial-up communications. Commenters indicated that physical security should only be required at Control Centers and High Impact substations with IP-based communications. While some commenters generally liked having all the Physical Security requirements in one standard versus references to multiple standards and multiple requirements within standards, the commenters expressed concern that the clarity that was intended was not provided, as the language used is vague and confusing. Some restructuring of the requirements was suggested to improve the clarity of the standards.

While some restructuring of the requirements for physical security has been implemented by the SDT in the Version 5 standards, each Responsible Entity is required to ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. CIP-006-5 defines the requirements for physical protection for Low, Medium, and High Impact BES Cyber Systems. While the requirements place the

emphasis for physical protection on the High and Medium Impact BES Cyber Systems, each Responsible Entity's Physical Security Plan is required to address how it will protect Low Impact BES Cyber Systems.

#	Organization	Yes or No	Question 15 Comment
15.1	National Rural Electric Cooperative Association (NRECA)		In R5.5, the statement to "Authorize unescorted physical access....." makes it sound like the utility should provide blanket authorization for unescorted physical access. I don't believe that is the case. Please clarify R5.5 -- I believe what is intended here is to have policies and procedures in place to detemine who has authorization to have unescorted physical acess.
15.2	Idaho Power Company		R6 is confusing. The headings suggest the need for a physical security plan but the tables pertain to requirements to protect physical access control systems. 6.1 should read "Restricting physical access to physical access control systems that are protecting BES Cyber systems identified in Requirement R5 Part 5.1, 5.2 5.3." 6.2 should read similarly. The current wording suggests that a physical access control system would be identified in Requirement 5 but it is not a BES cyber system because it does not perform a function listed in the attachment 1.
15.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.In R5 and R6, "prevent" is an objective (or purpose) and should not be embedded in the requirement, e.g., if unauthorized physical access occurs such as someone driving a bull-dozer through a building, is the entity non-compliant? Objectives should not be mixed with the actual requirement.In the bullets to R5 and R6, the areas in and of themselves do not "protect" BES Cyber Systems, they "contain" them.R5The requirement to "apply criteria" is not a strong requirement. FMPA suggests: "Each Responsible Entity shall apply the security controls specified in CIP-011-1 Table 5 - Physical Security for BSE Cyber Systems."In the bullets, there is confusion among the terms "grant" and "authorize". "Authorize" is senior manager approval, "grant" is being given the key or card. The requirements should keep these two concepts clear. For instance, in 5.5, "authorize" should be changed to something like: "Grant unescorted physical access to areas containing BES Cyber Systems only to those who are authorized

#	Organization	Yes or No	Question 15 Comment
			such access". Also, in order for 5.8 and 5.9 to apply to Medium, then 5.5 needs to apply to Medium.5.7, 5.9 and 5.9 will be open to interpretation. If an employee was given key and card access, is revoking card access sufficient or both the key and the card?5.7 should apply to Medium5.8 and 5.9 should be combined and the time durations correlated with the impact level instead of Control Center vs. Facility.5.10 strike "access"R6The order of R5 and R6 seems backwards. It would seem development of the physical security plan (R6) should come before implementing the plan (R5)
15.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 12.
15.5	Independent Electricity System Operator	Disagree	- R5.1 in table 5 please define what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?- 5.3 and 5.4 should be consistent in
15.6	Reliability & Compliance Group	Disagree	: Putting data retention into a separate section of the standard is confusing without a reference. If you want to keep data retention separate, you should refer to the data retention rules in the standard. i.e. Retention rules for R5 can be found in section 1.4.1 and 1.4.3 of this standard.Also, visitor control should be included for medium impact systems as well. If not, why are we restricting access to those systems if we can routinely open the door for anyone to come in and wander around unescorted. One interpretation of this would be to have some employees given access rights and others would be daily guests who are not logged or monitored.
15.7	Regulatory Compliance	Disagree	5.7 - qualification should be made in regards to a service vendor that the 24 hour period should start once notice is received from their company.5.8 - prefer 7 day revocation deadline5.9 - prefer 7 day revocation deadline
15.8	USACE - Omaha Anchor	Disagree	A) Dislike that methods to achieve compliance were removed from standard and will be placed in a guidance document. Guidance documents aren't binding. B) 5.9 - how do

#	Organization	Yes or No	Question 15 Comment
			you revoke access when it was never formally granted in the first place?
15.9	Duke Energy	Disagree	a) We generally like having all the Physical Security requirements in one standard versus references to multiple standards and multiple requirements within standards. However, the clarity that was intended is not provided as the language is vague and confusing.b) The standard has eliminated terms like the Physical Security Perimeter, 6 wall boundary and Physical Security Plan but it appears that they will be expected in order to achieve compliance. In fact, R6 includes a reference to "...one or more physical security plans..." that is not mentioned in the R5 requirement which appears inconsistent since R5 is the Physical Security for the BES Cyber Systems. Provide clarity and make consistent. c) Requirements 5.1, 5.2 and 5.3 appear to be less prescriptive than previous CIP 006 versions. However, is it left up to the Responsible Entity to determine the requirements for controlling access, monitoring access and logging access? Are some of the expectations from previous CIP 006 Rev. 3 still expected, but not documented? d) General Comment: V4 is very vague and unclear as to what is required. We would suggest additional wording to provide clarity as to what is intended for the responsible entity to physically meet R5.1, R5.2 and R5.3Physical security will be extremely difficult to implement on components located throughout the plant.For 5.9, assuming a key is used to access a system, revoking access within 72 hours maybe impossible. Changing locks may not be able to happen that fast. Face to face terminations may not be the case. Costs associated with card readers to replace locks is extremely high ($5-7k per reader, average 6 readers per hydro station and about 5 hydro stations this will apply to is a minimum of $150,000). Some systems are in cabinets that must be left open to do work. Card readers will set off alarms before work can be completed.For 5.11, should be deleted, as this should be included in the incident response procedures.For 5.2, what does monitoring entail?For 5.8, should be 48 hours.6.3 states "implementing maintenance and testing program....function properly". "Properly" is a vague term open for interpretation.
15.10	SCE&G	Disagree	Again, SDT should allow provisions for entities to leverage existing controls (i.e. Nuclear Facility Physical Security). NPP's have one of the most effective Physical Security

#	Organization	Yes or No	Question 15 Comment
			Programs of all Critical Infrastructures. CIP-011 R5/R5 should acknowledge this progam.5.2 SDT needs to better define what constitues appropriate "Monitoring". 6.3 "physical access control systems" should be defined. Is there an expectation for entities to walk fences around substations/generation facilities every 3 years?
15.11	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comment.
15.12	Liberty Electric Power, LLC	Disagree	CIP-011 R5 has very short times to revoke access. If an entity gives a contractor a code to enter the a room so he can download data on a Friday night shutdown, the code will have to be changed prior to the next business day -even if he is physically incapable of entering the plant.
15.13	E.ON U.S.	Disagree	CIP-011-1, R5.7, R5.8 and R5.9 does not fairly address the termination of access of contractors and/or service vendors. These types of requirements have generated many self reports to the NERC regions, and it is clear that this will continue so long as registered entities are presumed to have immediate knowledge of a change in the status of each contractor's employees. E ON U.S. proposes the requirements read as follows:R5.7 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for employees terminated for cause. For contractors/service vendors, access shall be revoked within 24 hours from the time of notification from the contracting/service vendor company."R5.8 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for employees who no longer require such access within 36 hours. For contractors/service vendors, access shall be revoked within 36 hours from the time of notification from the contracting/service vendor company."R5.9 - "Revoke authorized unescorted physical access to areas protecting BES Cyber Systems for employees who no longer require such access within 72 hours. For contractors/service vendors, access shall be revoked within 72 hours from the time of notification from the contracting/service vendor company."Additionally, CIP-011-1, R5.11 is ambiguous. E ON U.S. requests that the SDT clarify "review" to address is expected.

#	Organization	Yes or No	Question 15 Comment
15.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
15.15	LADWP	Disagree	Commensurate security measures need to be defined. If 6 wall is no longer the standard, what is replacing it?
15.16	Public Service Enterprise Group companies	Disagree	Comments: R5.8 requires physical unescorted access be revoked within 36 hours. This is too short a period, especially if the event occurs over a weekend or holiday. The timeframe should be changed to 5 calendar days or 3 business days. At a minimum, 72 hours.Physical protection of assets that are located within a NRC mandated Security Boundary / Perimeter that complies with NRC security regulations for Nuclear plants should be deemed to satisfy NERC CIP physical security requirements. NRC background checks, training, etc. for unescorted access and the physical security provided at Nuclear plants is more than adequate to satisfy NERC reliability physical security needs. Registered entities should not be required to implement duplicative procedures and programs for physical security of BES cyber assets located inside the NERC security Boundary/Perimeter. The drafting team should develop appropriate language to this effect.
15.17	CenterPoint Energy	Disagree	Disagree - For R5.8 and R5.9, CenterPoint Energy recommends increasing the timeframe for revocation of authorized unescorted physical access for personnel who no longer require such access to seven days as is found in the current Standard. CenterPoint Energy also believes physical access methods employed at a control center should differ versus those at a remote substation environment and therefore recommends revisions allowing for such differences.
15.18	FEUS	Disagree	Disagree with comments: 5.5 and 5.6 require authorization and quarterly reviews of unescorted physical access. It is not clear what type of authorization process would be required or what is required to be reviewed.

#	Organization	Yes or No	Question 15 Comment
15.19	Black Hills Corporation	Disagree	In 5.1, do not understand the significance of external connectivity only. Also in 5.1, restrict physical access is not defined (what evidence would be required to prove if we are not required to monitor, log, authorize, etc?) In 5.6, quarterly is a good goal, but without a solid definition of the window associated with "quarterly", this will be an evidence gathering problem - suggest changing to semi-annual. 5.2 & 5.3, and 6.2 & 6.3 should have consistent impact applicability.
15.20	Constellation Power Source Generation	Disagree	In R5.2, what is meant by the term monitor? Is that continuous, automated monitoring, or can it be an inspection during an operator's round? A suggestion would be to include the phrase "automated or manual" to add clarity. R5.4 defines the action of logging as "manual or automated." This definition should also be used in R5.3 and R5.2. In R5.6, why is the review on a quarterly basis? Other requirements ensure that a terminated employee has access revoked extremely quickly, so the review in R5.6 can be extended out to an annual review without an adverse reliability impact on the BES. In R5.9, why is the term generation lowercase? Is this implying a different meaning? R6.3 is requiring testing and maintenance of all physical security mechanisms on a cycle no longer than 3 calendar years. However, some plants are on a 3 to 5 year maintenance schedule and are otherwise expected to be running. This will force a plant to take an outage it otherwise would not have just to comply with a physical security requirement.
15.21	Luminant	Disagree	It does not make sense to physically protect BES Cyber System for Meduim Impact systems that have external connectivity. The impact of physical access is no different that for systems not externally connected. 5.8 change to 48 hours (2 days) 5.9 1 week. Also remove 5.8 and 5.9 from the Medium impact requirements, as you cannot revoke access since it is not a requirement to restrict or grant unescorted access.
15.22	Emerson Process Management	Disagree	It is unclear about the relevance of physical access control and external connectivity.
15.23	WECC	Disagree	Low and Moderate impact assets must have some baseline physical security. It appears

#	Organization	Yes or No	Question 15 Comment
			that some requirements have differences between the levels for their own sake without the justification of security risk analysis. The standard should be adjusted to provide baseline physical security for all systems regardless of impact and/or method of communication.
15.24	Manitoba Hydro	Disagree	Manitoba Hydro does not agree with the drafting team approach to defer the FERC Order 706 directive for multiple physical security perimeters. Upgrading physical security at facilities is costly and time consuming and deferring the multiple perimeter requirement will require entities to later rework physical security at many facilities. The drafting team should either include the multiple physical security perimeters in version 4 or limit all physical security requirements to those already completed under CIP V1-V3. The reference in Requirement R5.11 to incident response procedures should be cross-referenced to Requirement R27, assuming that these are the procedures being referenced in Requirement R5. Requirement 5.7 could be interpreted as a subset of Requirement 5.8. Requirement 5.8 should explicitly exclude personnel terminated for cause. There are no specifics given with respect to 'restricting' access in Requirement 6.1 so it is assumed to be at the Responsible Entity's discretion in terms of to whom, by what means, etc. It is not clear if the "Required for routable access only" in the impact columns refers to routable BES Cyber Systems or routable physical access control systems.
15.25	Network & Security Technologies Inc	Disagree	Minimum retention period for logs should be specified. 5.11 does not specify a time frame for reviewing and handling unauthorized physical access attempts.
15.26	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R5, but recommends changes as follows: o Regarding Table R5, Minnesota Power recommends changing "areas protecting" to "areas containing BES Cyber Systems" to reduce ambiguity and confusion. o For Section 5.1 of Table 5, for Medium Impact Systems, the inclusion of the term "external connectivity" as a qualifier that creates confusion. The relevance of connectivity to implementing appropriate physical security measures is not clear. Physical Access averts the need for electronic access, so this seems

#	Organization	Yes or No	Question 15 Comment
			counterintuitive to include “external connectivity” as a provision. Minnesota Power recommends that the reference to “external connectivity” be removed from sections 3.2, 4.2, and 5.1 of Tables 3, 4, and 5 respectively. o As currently written, sections 5.3 and 5.4 seem to be similar and could be combined. If it is the Standards Drafting Teams intent that 5.3 apply to those individuals authorized for access, then Minnesota Power recommends the following revision to R5.3:"Log physical access to areas containing BES Cyber Systems for individuals with authorized cyber access and/or authorized physical access. Logging should..." o For sections 5.5, 5.6, 5.7 and 5.10 Minnesota Power recommends that the Medium Impact column match section 5.1. Since 5.1 requires restricted access, that implies that authorization needs to exist for access as well as access review, revocation, and visitor escorting procedures.Minnesota Power generally agrees with the proposed Requirements R6, but recommends changes as follows: o Requirement R6 discusses preventing and/or detecting unauthorized physical access to BES Cyber Systems while the sections of Table 6 discuss “physical access control systems.” This inconsistency creates confusion regarding what should be included in the physical security plan(s). o Regarding Table R6, Minnesota Power recommends changing “areas protecting” to “areas containing BES Cyber Systems” to reduce ambiguity and confusion. o Parts 6.1, 6.2, and 6.3 of Table 6 refer to the “physical access control systems” identified under Requirement R5, Part 5.1, 5.2, 5.3,” but R5 does not identify or use the term “physical access control systems.” Rather, it requires restricting, monitoring and logging physical access and does not require an access control system to do so. Certainly, as a result of its analysis and implementation of Parts 5.1, 5.2 and 5.3, a Registered Entity may implement an electronic system for access control, monitoring and logging, but it is not explicitly required. These parts should be reworded to state that if the Registered Entity has implemented an electronic physical access control system, then these requirements apply.
15.27	NextEra Energy Corporate Compliance	Disagree	NextEra believes it is not specifically clear what relations the different requirements have for the Medium Impact BES systems. For example, 5.1 requires that physical access be restricted, however, it would appear that this access does not need to be logged, authorized, or reviewed in 5.4 through 5.6. Similarly, 5.9 requires revocation of this

#	Organization	Yes or No	Question 15 Comment
			restricted access which may not have been authorized. We believe that R5 needs further clarification.Also, provide clarity regarding 5.1 "External connectivity only" requirement in Medium Impact column. For a site with Medium Impact BES Cyber systems, why would access not be restricted only if the BES Cyber Systems had no external connectivity. Granting access to the site may result in same impact once the individual is at the site as if they had remote connectivityRegarding R5 & R9 - 24 hour revocation requirement “for cause”, technical infrastructure does not support wide scale user administration to revoke cyber access within 24 hours. User administration for site cyber devices is not centralized. NextEra suggests providing specific definition of “revocation of access” to specify physical / cyber access. For example, if an individual has cyber access only and physical access and remote access to the systems is removed, this effectively revokes access. Regarding R5 & R9, what triggers “for cause” termination / no longer requires access?There needs to be consistency of administration in the industry. What starts the 24 hour clock?NextEra believes it should be at the point where the decision is officially entered into the system and/or communicated to the individual no longer requiring access.
15.28	Consultant	Disagree	NOTE: The format of these two requirements and tables is better than that for Requirements R1 through R4. For R5 & R6 the 'requirement' states the objective and the table specifies the required activities.R5 & R6 - The wording to implement the criteria in the tables is incorrect. The tables are specifying the requirements and application of requirements to the classes of assets resulting from the impact categorization process. The wording of the statement should be modified to reflect this distinction.R6. A physical security plan does not "prevent or detect unauthorized physical access..."It appears that R6 is misidentified as Physical Security Plans, when it seems to address protection for cyber systems providing physical protection to BES Cyber Systems.Based on the reconfiguration of the requirements in this standard a physical security plan is not necessary to meet the requirements.Suggest this requirement be restated to replace the term "Physical Security Plans" with "Protect Physical Access Control Systems" Table item 6.1 would require protection of cyber systems performing the functions identified in Table R5 items 5.1, 5.2, and 5.3 (See next comment regarding deleting 5.2).Table item

#	Organization	Yes or No	Question 15 Comment
			6.2 would require protection of cyber systems performing logging functions for physical access points.Table item 6.3 would require implementation of a maintenance & testing program for the assets identified in 6.1 & 6.2.A better option would be to include in Attachment 1 a function that relates to physical access control systems as part of the BES Cyber System identification. Such as:Physical Access Controls - activities, actions and conditions necessary to restrict and to log physical access to BES Cyber Systems. This would allow items 6.1 & 6.2 to be deleted, and the protections for "BES Cyber Systems" to apply to the physical access control cyber systems. Should the maintenance and testing requirements apply to BES Cyber Systems identified during the identfication and categorization proces, including those that are used to control physical access?
15.29	Garland Power and Light	Disagree	o Requirement 5.10 - clarify that continuous escort does not include entering bathroom facilities - some bathrooms are small non-partitioned one room facilities and it is inappropriate for escort in such areas.
15.30	PacifiCorp	Disagree	PacifiCorp generally agrees, except R5.9 should be expanded to control centers as well, and R5.8 should be removed. There is not a significant or compelling reason for different deadlines which add to the complexity of the standards and the administrative workload to parse the circumstances of each revocation.Define Physical Access Control Systems and ensure the controls in others requirements are suitably applied to those components.
15.31	Progress Energy (non-Nuclear)	Disagree	PE agrees with the 24 hour timeline for access revocation for employees terminated for cause, however it believes this will continue to pose a considerable challenge to many in the industry for its contractor population and would suggest “upon notification” be added to the beginning of the sentence. Thus, Section 5.7 would read, “Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for personnel terminated for cause.”PE disagrees with content set forth in R5.8 and R5.9 and believes it will be difficult for many entities to meet and likely result in significant violations throughout the industry. PE suggests language be added to include “upon notification” for both sections and change 36 hours to 48 hours

#	Organization	Yes or No	Question 15 Comment
			for Control Centers so that Section R5.8 reads: "Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 48 hours," and Section R5.9 reads: "Upon notification, revoke authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 72 hours."5.1 implies that we could have a cyber component without external connectivity. 5.7 revocation of access within a 'hours' timeframe implies that the access would be controlled through a security group with 24/7 coverage. Other requirements appear to be in line with requirements of previous standards.CIP-011 R5.7 thru .9 what is the decision process to be used to determine "when job duties no longer require ... access"? What would be suitable compliance evidence that is to be collected that indicates "when job duties no longer require access" as this is critical in determining if revocation has been accomplished within the mandated 1 hour, 4 hours, 6 hours, 24 hours, 36 hours, 72 hours?Need clarification on period allowed for revocation of access due to expiration of training of background check - recommend that this be included with 5.8, 5.9 (no longer require access - or fail to meet necessary criteria).R5.7 - poor wording "handle...access attempts" Propose: "process such physical..."
15.32	Allegheny Energy Supply	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.
15.33	Allegheny Power	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.

#	Organization	Yes or No	Question 15 Comment
15.34	EEI	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls.
15.35	MidAmerican Energy Company	Disagree	Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to determine the components that may need additional controls. Define Physical Access Control Systems and ensure the controls in others requirements are suitably applied to those components.
15.36	Oncor Electric Delivery LLC	Disagree	Physical security at remote substation sites is not cost effective in preventing/detecting cyber attacks. Remote substations with only dial-up communications cannot support the 24-hr time frame of Requirement 5.7 when systems are non-functional (phone line damage, etc). Five to seven days may be required, depending whether some communication system has been installed to the facility. Physical security should only be required at control centers and High impact substations with IP based communications.
15.37	American Electric Power	Disagree	Please see comments as provided in response to Question 15.
15.38	Puget Sound Energy	Disagree	Puget Sound Energy has the following suggested changes:Table 5:5.3 - Suggest changing to “Logging shall record sufficient information to uniquely identify known individuals, or assist in the identification of unknown individuals, and the time of access...”Table 6:6.1/6.2 - Puget Sound Energy would like clarity on how restricting physical access to areas protecting control or monitoring systems for physical access protects the BES Cyber Systems. Physical protection of the BES Cyber Systems (Table 5) is understandable to protect the BES. But, a malicious or inadvertent act solely against the Cyber Systems that provide physical security in no way impact the BES or the Cyber Systems that make

#	Organization	Yes or No	Question 15 Comment
			up the BES unless the physical location of both types of Cyber Systems is the same.6.3 - Puget Sound Energy requests clarity on "...of all physical security mechanisms...". Like many entities, Puget Sound Energy employs physical security measures that are made up of components that do not use routable protocols. Is 6.3 suggesting a full test of all mechanisms (routable protocol or not) involved in restricting, monitoring, and logging? (Ex: card key strikes at doors)
15.39	LCEC	Disagree	R5 - and/or should simply read or. "To prevent and/or detect unauthorized physical access" should read "limit access to authorized personnel through detection and prevention."Medium impact for "external connectivity only" doesn't make sense from a physical security perspective. Change to Control center only.Move 5.8 and 5.9 to 5.7 and base the timings on whether or not it is a control center. CC should be 36 hours and others should be 72 hours.5.5 should be required for Medium as well since there is a requirement to revoke access in 5.8 & 5.9The term "areas protecting" is confusing and should be replaced with "areas containing" BES Cyber Systems.Please consider identifying at what level of access granting must be removed to sufficiently mitigate the personnel risk.R6 Need to clarify "required for routable connectivity only" in regard to physical security controlsMost physical security systems do not require preventive maintenance which makes it difficult for an entity to provide a basis for maintenance performed. Testing is also a challenge because these systems either work or they do not work. What is the intent of the testing and maintenance requirement? Can this requirement be better served by reviewing the configuration of the system and comparison to approved access lists?
15.40	Southwest Power Pool Regional Entity	Disagree	R5 does not address the expectations of FERC Order 706 and subsequent orders. 5.3 needs to include both ingress and egress. 5.4 needs to include identification of the escort staff. 5.3 and 5.4 could be combined. 5.7: The time to revoke physical access can be much faster for control center environments; suggest 2 hours for the control center and 8 hours elsewhere. Ideally, the person's primary access credentials (badge, keys, etc.) should be lifted and access revoked concurrently with the person being notified of the termination for cause. 5.8 and 5.9 can be combined and the timeframe should be

#	Organization	Yes or No	Question 15 Comment
			expressed in business days. 5.10: define "continuous escort" somewhere. R5 overall: consider defining the concept of specifying an "effective date" of a transfer that reflects the reality that often a transferred employee will back fill or support the losing department for a period of time after the HR date of the transfer. 6.3 needs to be much more frequent in a control center environment where the inspection program can be readily performed; weekly is suggested. Additionally, the frequency needs to be commensurate with the impact category regardless of site characteristics.
15.41	ISO New England Inc	Disagree	R5.1 in table 5 please defined what is meant by external connectivity. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary?R5.8 and 5.9 Is the 36 hours or 72 hours from the time the access is reviewed? Or is it that access should be reviewed within 36 hours of personnel that change job responsibilities, transfer, etc. Then require access be modified based on the review. Suggest changing the 36 hours to 72 hours. If a transfer were to occur on a Friday at 5 pm then access would need to be reviewed by Sunday.
15.42	Western Area Power Administration	Disagree	R5.2: What is the definition of "monitoring" physical access? Since the concept of the physical security perimeter has been dropped, what specifically is meant by "access to areas protecting BES cyber systems? What constitutes sufficiency in monitoring?R5.3: What constitutes sufficient logging? Is a self-written logbook sufficient? Does logging have to be performed electronically or by a third party if manually logged, or is self-logging sufficient?R5.5: How does 5.5 differ from the requirements of R4?R5.7: Can be very difficult if someone is terminated on a Friday afternoon. Communication is very critical and requires more people knowing in advance, which in itself may cause an additional risk. R5.8: 36 hours could be an issue on 3 day weekends. Suggest 48 hours. Then is will only be an issue at Thanksgiving.R6, 6.3: Needs more guidance on testing and maintenance program what they must cover besides a blanket statement of testing and maintenance of all physical security mechanisms. Shouldn't we follow the installers or manufacturers recommendation on this? Documentation of these tests and maintenance evidence should be kept for how long?R6: what is meant by "routable

#	Organization	Yes or No	Question 15 Comment
			connectivity only"?
15.43	Kansas City Power & Light	Disagree	R5.3: What does "sufficient information" mean? This may encourage too much interpretation and recommend some clarity in the Table R5.R5.10: How do you prove someone who requires an escort was escorted at all times? From an audit perspective this is "proving the negative". It is understood what is intended in this requirement, but this is not measurable or auditable.R6.1 through R6.3: qualification here of "routable connectivity only" is not clear with respect to physical access controls. Routable implies electronic security measures rather than physical.
15.44	Con Edison of New York	Disagree	R5.8 and R5.9 - Add the words "Required for" before "Control Center" or before "Generation or Transmission Facility".R5.1 Need clarification to this item. If I have an enclosure which secures and isolated my cyber system, do I need to restrict access into the enclosure or do I need to restrict access to the area around the enclosure?R5.6 - Quarterly reviews are excessive. Annual or bi-annual would be reasonable.R5.9. - Should be business days, for example 3 business days. Support staff may not be available 24/7 to do this work.R5.10 - Continuous escort access is not practical in the numerous substations. The requirement should be relaxed to say oversight or supervisor, or any other mean which will limit the total escort and allow the operator to perform tasks while people may come to the station.R5.1 Medium Impact; not sure what external connectivity means? R3 clarification may resolve this.R5.8 (and others) - 36 hour requirements for compliance criteria will be a challenge
15.45	San Diego Gas and Electric Co.	Disagree	R5.8 and R5.9 require revoking authorized unescorted physical access to areas protecting BES Cyber Systems for personnel who no longer require such access within 36 hours for medium and high impact control centers and within 72 hours for medium and high impact generation or transmission facilities. CIP-006-2 R1.5, by reference to CIP-004-2 R4, currently requires such revocation within 7 days for all PSPs. Revocation within 36 or 72 hours will be much more difficult to capture, especially for internal personnel reassignments. SDG&E believes that the risk to BES Cyber Systems associated with reassignment of an employee does not justify the effort (and potential non-

#	Organization	Yes or No	Question 15 Comment
			compliance) associated with this change. These time-periods approach the 24-hour limit for personnel terminated for cause in CIP-006, which does carry genuine risk to BES cyber systems.R6.1 and R6.2 in CIP-011-1 concern restricting and monitoring physical access to "areas protecting physical access control systems". Does this mean areas equivalent to PSPs have to be set up around these physical access control systems? Currently, CIP-006-2 R2 and R2.2 concern protection of "cyber assets that authorize and/or log access" to PSPs. Thus, server racks and control panels are locked and monitored, but PSPs are not required around these systems.
15.46	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R5.8 and R5.9 should be extended to 72 hours or next business day, whichever is longer, to allow for communications for this circumstance. A late Friday occurrence could be addressed early Monday instead of over the weekend.
15.47	Dominion Resources Services, Inc.	Disagree	R5.8 and R5.9. To meet regulatory directives, if job duties are changed due to disciplinary actions or are "forced" on the user, then a shorter time frame to revoke access may be necessary. However, the current 24 hour time period is the least time period that can be reasonably accommodated through the business processes.Requirement R4 establishes the process for personnel risk assessments. This practice determines the loyalty, reliability and trustworthiness of an individual as a prerequisite to authorizing logical or physical access. This is a standard practice used throughout the physical and cyber security industry and accepted by other regulatory agencies and Federal programs. Similar to R4.3, personnel risk assessments typically must also re-validate this trustworthiness periodically - commonly within 7 years and in some cases more frequently depending on the nature of the access. The presumption is that, once trustworthiness is established, it is not invalidated unless there is cause to reconsider or an individual voluntarily terminates their employment or retires. Only in instances where the established trustworthiness is in question, is prompt access revocation appropriate and warranted. Consequently, for personnel who "no longer require access", but for which there is no cause to question their trustworthiness, there is no basis for immediate or prompt revocation of access within the time frames

#	Organization	Yes or No	Question 15 Comment
			specified in this standard. The DHS Catalog for Control System Security Controls, Sections 2.3.4 and 2.3.5 reflect this practice - requiring revocation of access for cause within 24 hours and revocation of access for personnel reassigned or transferred to another position within 7 days. In other regulatory programs, revocation of access, not involving a question of change in trustworthiness, is handled via a periodic (e.g., monthly) review of access only. The 7 day requirement in the current standards would meet or exceed standard practice in this case. The requirements should be clarified to state that if there is no triggering event indicating that access is no longer required, then that determination should be made at the quarterly review.
15.48	ERCOT ISO	Disagree	Recommend moving requirements 5.5 through 5.9 to a common access management section which addresses cyber access and information access. The remaining parts of Requirements R5 and R6 could be combined.
15.49	US Bureau of Reclamation	Disagree	Requirement R5: Physical security requirements are not adequately addressed in the present Standard. Much of the language from the previous version of the Standard should be re-established in version 4. In addition low and medium systems should include the equivalent of a 6-wall boundary around the cyber systems.Requirement R6: Physical security plans should be required for more than just electronic physical access control systems.
15.50	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
15.51	Xcel Energy	Disagree	The 36 and 72 hour timeframes to revoke unescorted physical access for individuals no longer requiring access under 5.8 and 5.9 are not justified. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not needed. "Restrict physical access" in Requirement 5.1 also needs further definition. Does this mean locks?

#	Organization	Yes or No	Question 15 Comment
			Fencing?There appears to be inconsistencies between R5 and R6. Specifically;1) Table R5, R5.1 applies to Medium impact systems with external connectivity, while Table R6 6.1 applies to Medium impact systems with routable connectivity. 2) Table R6 refers back to 5.1, 5.2, and 5.3 for Medium impact systems, however 5.2 and 5.3 do not apply to Medium impact systems.
15.52	GTC & GSOC	Disagree	The 36 hour requirement for a person who no longer needs access (R5.8) is too stringent. If a transfer or retirement occurs on a Friday there is no reason you cannot wait until Monday. We recommend changing this to "within 36 hours or the next business day, whichever is greater".
15.53	APPA Task Force	Disagree	The APPA Task Force recommends the following edits to R5-R6:R5. Objective:To prevent and/or detect unauthorized physical access to BES Cyber Systems.R5. Requirement:Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R5 - Physical Security for BES Cyber Systems." R6. Objective:To prevent and/or detect unauthorized physical access to BES Cyber Systems.R6. Requirement: Each Responsible Entity shall document and implement one or more physical security plans that apply the criteria specified in CIP-011-1 Table R6 - Physical Access Control Plans
15.54	Bonneville Power Administration	Disagree	The objective of these requirements ("to prevent and/or detect unauthorized physical access to BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action(s) that the Responsible Entity must take.The objective of R5 and R6 should be changed to read "to prevent and detect unauthorized physical access to BES Cyber Systems." They should not say "and/or". Isn't the objective to prevent unauthorized physical access to BES Cyber Systems and to detect unauthorized physical access to BES Cyber Systems?R6: The entries in Table R6 refer to "Part 5.1, 5.2, 5.3". It is unclear whether these refer to subrequirements R5.1, R5.2, and R5.3, which do not exist, or in Table R5, entries 5.1, 5.2, and 5.3.5.7-5.9 refer to timeliness of revocation. Twenty-four hours for terminations for

#	Organization	Yes or No	Question 15 Comment
			cause is reasonable, however having two additional categories complicates matters and could potentially lead to confusion and someone not revoked in the appropriate category. For 5.8-5.9 this should be the same and be reviewed to take place within 3-5 business days. 5.11 is good in that unauthorized physical access is a procedural violation and not necessarily an incident.
15.55	Exelon Corporation	Disagree	The requirement to revoke access (5.8 & 5.9) in 36/72 hours for personnel who no longer require access is far too severe and places unnecessary administrative burden on the entity without technical or risk analysis justification. This would imply that there is little differentiation between an employee terminated for cause and a person who we regard as a solid member of our organization and in turn, we deem as having integrity. This would also become an undue burden to the business as our employees require transition time to ensure there is reliable transfer of information to the new owner of a role or task. This requirement would make that transition period extraordinarily difficult. Also, the ability to capture and store the transfer data to the hour would be impossible with our current human resource data systems. Modifying this system would result in major expense with little to no stated benefit to BES reliability. Exelon's position is that the current 7 day requirement is reasonable from a technical and risk perspective. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
15.56	Ameren	Disagree	The short period of time to remove access for 5.8 does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that this requirement be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred. Also, R6 should be a stand alone requirement, remove circular reference to R5.â€,
15.57	Pepco Holdings, Inc. -	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 15 Comment
	Affiliates		
15.58	Entergy	Disagree	We disagree with 5.1 "Restrict physical access to areas protecting BES Cyber Systems" for Medium Impact BES Cyber Systems with external connectivity only. What difference does it make if the physical security of Medium Impact BES Cyber Systems access is restricted to the Physical Security Perimeters if the access mode to be protected is external, but there is no other requirement to monitor, or log access into or out of the PSP for these cyber systems.How can access be revoked from a Medium Impact BES Cyber Systems if there is no requirement to monitor or log access in and out of the PSP? There seems to be conflict with these requirements. Remove the requirements 5.1, 5.7 and 5.8 for Medium Impact BES Cyber Systems.Instead of having different access revocation time frames for High Impact BES Cyber Systems based on the locations as described in requirements 5.7, 5.8 and 5.9 it would be easier to manage evidence for compliance if all locations was the same. During the Dallas CIP Workshop it was apparent that the SDT was struggling with the interval for access revocation. It is suggested that the revocation of physical access for employees terminated for cause be by the end of the business day the first normal business day after the employee is terminated i.e. if the entities normal business week is Monday - Friday 8:00 - 5:00 and an employee is terminated Friday to Sunday then revocation should be completed prior to 5:00 on Monday for all High Impact BES Cyber Systems regardless were the cyber systems is located, control center, transmission facility or generating station. This would provide a consistent method of tracking the access revocation across the entities facilities and reduce requirements and potential compliance shortcoming and reduce the vulnerability of not taking actions to terminate employees for cause if the 24 hour requirement cannot be achieved on the weekend and the termination be held off until the normal work week when the requirement can be met.
15.59	We Energies	Disagree	We Energies agrees with EEI comment: Physical Access Control Systems need to be defined. The term will have different meanings for different entities and auditors. It will be difficult to implement and audit without a definition in place. Physical Access Control Systems will require additional controls in other standards. Specificity is required to

#	Organization	Yes or No	Question 15 Comment
			determine the components that may need additional controls.
15.60	PNM Resources, Inc.	Disagree	We would prefer that all accress granting and revocation, for physical and logical access, be identified in a single table. In the current draft, they are scattered through several unrelated requirements.

16. Tables R5 and R6 provide direction concerning what impact level of BES Cyber Systems to which Requirements R5 and R6 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Some commenters expressed concern that the electric industry already physically protects its cyber assets from the public for reliability, business, and safety reasons, and that making physical security a standard requirement for Low Impact BES Cyber Systems creates an additional compliance burden that does not contribute any additional reliability to the Bulk Electric System.

Each Responsible Entity is required to ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. The SDT has revised CIP-006-5 R1 to define the requirements for physical protection for Low, Medium, and High Impact BES Cyber Systems. While the requirements place the emphasis for physical protection on the High and Medium Impact BES Cyber Systems, each Responsible Entity's Physical Security Plan is required to address how it will protect Low Impact BES Cyber Systems.

Some commenters also expressed concern that there appears to be a discrepancy in the Medium Impact category, where there could be sites that are not required to restrict access because there is no external connectivity, but they are required to revoke access. The SDT has revised these requirements and has removed the consideration for external connectivity from the applicability portion of this requirement, such that all Medium Impact BES Cyber Systems are required to have a Physical Security Plan. The revocation of access requirements are enumerated in CIP-005-5 R7, and have eliminated the identified potential for conflict.

Some commenters expressed disagreement with the requirements for restricting, monitoring, and maintenance testing for systems that provide physical access control over Medium BES Cyber Systems, when there is no requirement to monitor or log access into a Medium BES Cyber System. This likely is a conflict with the requirements for Medium BES Cyber Systems. The tables need to document basic physical security requirements for all Low and Medium Impact BES Cyber Systems. The SDT has revised the requirements for physical and electronic access for Low, Medium, and High Impact BES Cyber Systems to address these concerns. These requirements are stated in CIP-005-5 and CIP-006-5.

#	Organization	Yes or No	Question 16 Comment
16.1	American Municipal Power		Please provide a little or no impact category.
16.2	Regulatory Compliance	Agree	BUT:5.1 Medium Impact - "Required" only.

#	Organization	Yes or No	Question 16 Comment
16.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Blanks are ambiguous. If Low Impact is “Not Applicable”, then the blanks should be replaced with “NA”FMPA recommends making more clarity to the terms “required for external connectivity only” or “required for routable connectivity only” with: “required for areas containing BES Cyber Systems with routable external connectivity”FMPA believes that even Low Impact BES Cyber Systems should have restricted physical access and believes 5.1 ought to be applicable to Lower Impact “for areas containing BES Cyber Systems with routable external connectivity”R6 assumes card access and a “physical access control system” where the physical access may be restricted through lock and key (especially in substation environments for Medium Impact) and monitored through an alarm signal of a substation control house door opening through a SCADA system. It is unreasonable to require testing of simple padlocks or door-locks in 6.3.Maintenance of such system in 6.3 is unreasonable. Such electronic systems are usually just tested on a periodic basis and maintained as necessary. And, we assume that use of the system is testing the system. If not, what type of testing would be required in 6.3?
16.4	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
16.5	Manitoba Hydro	Agree	Manitoba Hydro agrees that physical security is not a standard requirement for Low Impact BES Cyber Systems, and should not be auditable. The electric industry already physically protects its cyber assets from the public for reliability, business and safety reasons. Making physical security a standard requirement for Low Impact BES Cyber Systems creates an additional compliance burden which does not contribute any additional reliability to the Bulk Electric System.
16.6	San Diego Gas and Electric Co.	Agree	Most of the requirements in Tables R5 apply to “high impact” BES cyber systems. Table R6, dealing with physical access control systems, applies to medium impact systems with

#	Organization	Yes or No	Question 16 Comment
			routable connectivity and high impact systems. This seems reasonable, but the scope will depend on what SDG&E determines will fall into these impact levels. Except as noted in the comments for Question no. 15, there are no apparent increases in physical security requirements for covered systems.
16.7	NextEra Energy Corporate Compliance	Agree	NextEra agrees but would like clarification regarding "Required for routable connectivity only" on Medium Impact physical access control systems. Also, as written, the standard does not have consistency in application of the different requirements as noted above.Also, in 5.11, how is the "unathorized physical access attempt" defined? Should this apply to all attempted access card swipes for electronic access systems. We do not believe that application of the incident response plan should apply to attempts such as these at the physical boundary. We believe a tie to suspicious activity threshold or physical boundary damage may be a better definition.NextEra also questions table R6, do training and PRA requirements apply to individuals with access to Physical Access Control Systems for BES Cyber Systems?
16.8	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 12.
16.9	Northeast Utilities	Agree	Suggest merging 5.8 and 5.9 and using 72 hours for the allowable revocation period for all personnel terminated not for cause.
16.10	Minnesota Power	Agree	With the implementation of the changes and clarifications described in Question 15, the impact levels seem reasonable.
16.11	Independent Electricity System Operator	Disagree	- For R 5.8 and 5.9, if restricting physical access is not required for Medium impact assets (R5.1) then why does access need to be revoked?
16.12	PacifiCorp	Disagree	: PacifiCorp agrees with EEI's observations below:Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.Table R5

#	Organization	Yes or No	Question 16 Comment
			Row 5.2: There should be additional language describing what “Monitoring” means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.Table R6 Row 6.3, it is appropriate to validate those basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.13	Madison Gas and Electric Company	Disagree	: Recommend 5.3 to use the same wording as 5.4 concerning logging access. This would reduce any confusion and provide uniform outcome to each sub requirement. Recommend 5.3 to read:”Log (manual or automated) ...” 5.7 states “Revoke authorized unescorted physical access to areas protecting BES Cyber Systems within 24 hours for personnel terminated for cause”. It may be possible to turn off someone’s electronic access but if there are combination locks, key locks, etc, this may not be possible to accomplish within 24 hours. This also applies to 5.8 and 5.9..
16.14	National Grid	Disagree	1. 5.1 - for Medium Impact BES CS, is it external connectivity with both routable and non-routable protocols? Please specify.2. There appears to be a discrepancy between 5.1 vs 5.7 & 5.8 in the Medium impact category. There could be sites that are not required to restrict access per 5.1 because there is no external connectivity. But, they are required to revoke access per 5.7 & 5.8. Could this be clarified?3. Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9.4. In 5.11, is the SDT considering providing the timeline for reviewing any unauthorized physical access attempts?5. Should the “routable connectivity” be “external connectivity” or “external routable connectivity” for Requirements 6.1, 6.2 and 6.3?
16.15	Consultant	Disagree	5.1 Physical access "Required for External Connectivity Only" is not logical. Suggest rewording to clarify.It is not clear why the change from Physical Security Perimeter to

#	Organization	Yes or No	Question 16 Comment
			the words "areas protecting BES Cyber Systems" makes sense. The new wording is not as clear and removes what was a "bright line". Suggest retaining the Physical Security Perimeter term in this version of the standards. 5.3 As this is currently stated it would appear to require monitoring and logging of both ingress & egress from "areas protecting BES Cyber Systems". Based on the discussion at the workshop, this is not the intent of this requirement. If that is the case then the wording should be modified to reflect the intent. 5.2 and 5.3 The distinction between "logging physical access" and "monitoring physical access" is not clear. If access is logged, then by default it has been monitored. Suggest deleting 5.2, or clarifying the difference between monitoring and logging in this context.5.4 The parenthetical after the word visitors is a definition, and as such should be listed as a definition, rather than being embedded in the requirement statement.5.4 Suggest replacing "to and from" with "entry and exit" or "ingress & egress". A more logical sequence of the requirements list by topic flow would be 5.1, 5.5, 5.3,5.2(see above comment), 5.4, 5.10, 5.7, 5.8, 5.9, 5.6.5.7, 5.8, 5.9 - Personnel transactions are typically measured in days. Setting a requirement in hours for a transaction that is not recorded at that level will create compliance problems. Suggest checking with the nuclear industry about time frames for access revocation. The answers there would be based on over 30 years of regulatory scrutiny.5.8 & 5.9 - There is no difference for personnel transactions based on the facility type, so creating a differential time frame for revocation by facility type would seem to imply that some facilities have less impact than other facilities outside of the impact categorization criteria. Suggest the access revocation time frames should be consistent based on the impact categorization, or adjust the impact categorization criteria to be consistent with the listed revocation time frames. The current table would imply that control center are high impact, and generation and transmission facilities are medium impact.5.11 Suggest deleting the word "any" as the current wording is unnecessarily restrictive. For example, the current wording implies that a single "bad swipe" of an access card should be reviewed, while entities typically have defined 3 to 5 consecutive bad swipes as an adverse event.5.1, 6.1, 6.2 & 6.3 - These table items create another dimension to the impact categorization process. If an asset has been categorized as Medium Impact, it should be afforded the

#	Organization	Yes or No	Question 16 Comment
			same level of protection as any asset categorized as Medium Impact. If the asset does not require the same level of protection then the impact categorization criteria should be adjusted to have it excluded from that impact level.
16.16	US Army Corps of Engineers, Omaha Distirc	Disagree	5.1 unclear why medium impact for "required for external connectivity only." Does this only apply to external connectivity hardware or is it for systems with external connectivity only? 5.8 & 5.9 are inconsistent with 5.5 granting of access is not required for Medium impact BES Cyber Systems.
16.17	Reliability & Compliance Group	Disagree	5.1, 5.5 and 5.8 are contradictory. They make you restrict and revoke access to medium impact systems but how do you do that if you don't have to authorize access to medium impact systems?Also, table R6 contradicts table R5 with regard to medium impact systems.
16.18	ERCOT ISO	Disagree	5.1: Please clarify why "Required for external connectivity only" is specified for medium impact BES Cyber System. 5.2-5.7: Should apply to medium impact BES Cyber System.5.10-5.11: Should apply to medium impact BES Cyber System.6.1-6.3: Please clarify why "Required for external connectivity only" is specified for medium impact BES Cyber System.
16.19	Dairyland Power Cooperative	Disagree	5.11 seems to say that known physical security incidents can be ignored for low and medium impact systems. This seems wrong. If a non-routable protocol terminates at some other facility, it seems there potentially should be physical access controls for that other facility as well-perhaps this would be required for high impact systems.
16.20	LCEC	Disagree	5.5 should be required for Medium as well since there is a requirement to revoke access in 5.8 & 5.9R6 Need to clarify "required for routable connectivity only" in regard to physical security controls
16.21	Duke Energy	Disagree	a) CIP-011-1 Table R6 is identified as applying to "Physical Access Control Systems" but is very confusing to understand as written because the columns describe levels of impact

#	Organization	Yes or No	Question 16 Comment
			to the BES Cyber System but there are no impacts if the Physical Access Control System is operated on a network that is separate and distinct from the SCADA system. Is that the intended interpretation?b) Table R5 Physical Security for BES Cyber Systems state that requirement 5.1 applies only to Medium Impact BES Cyber Systems with "...External Connectivity Only". Does this mean that since 5.1 only requires restricting access to BES Cyber Systems; an acceptable method would be mechanical lock and key control?c) Table R6 Physical Access Control Systems state that Medium Impact BES Cyber Systems requirements R6.1, R6.2 and R6.3 for physical security are "Required for Routable Connectivity Only". Does this mean "Routable Connectivity" of the BES Cyber System or Physical Access Control System?d) Was the access control system intended to be included or intended to be excluded if it is on a separate network and not connected with any BES Cyber Systems? e) General Comment: V4 Tables R5 & R6 are very vague and unclear as to what is required. We would suggest additional wording to provide clarity as to what is intended for the responsible entity to physically meet R6.1, R6.2 and R6.3For Table R5, we propose the addition of "for external connectivity only" in the high impact column. Same for Table R6. Suggest changing "routable" in the table to "external" in Table R6Remove requirement for Medium impact in 5.1. Remove requirements for Medium Impact Systems in Table R6Requirement R6, Medium Impact: allowances should be included to exclude BES cyber systems which incorporate one way connectivity (e.g. outside the ESP via a one way hardware device), even if the protocol is routable. This would be in addition to the existing non-routable protocols.
16.22	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.5.8 - 5.10 is the first of many occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any

#	Organization	Yes or No	Question 16 Comment
			distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
16.23	Southwest Power Pool Regional Entity	Disagree	At a minimum, access revocation should extend to all impact categories. Access to a BES Cyber System is an available attack vector. 5.2: Restricting access without monitoring access is an ineffective control; 5.1 is not auditable in the absence of some sort of verification that the control is in place. 5.3 needs to consider that automated logging systems cannot guarantee 100% up time. Consider adding a requirement for recognizing the automated process has failed and responding to the failure (not the same as repairing the failure, which will be situation dependent. 5.11: There should be a clearly defined maximum timeframe for reviewing unauthorized access attempts. Simply leaving it to the discretion of an entity's incident response plan is not an effective control. R6: The Cyber security plan applicability will need to be updated to reflect any changes to the R5 applicability matrix.
16.24	US Bureau of Reclamation	Disagree	At a minimum, physical security controls should be required for low and medium systems, even if it is just a lock on the door.
16.25	FirstEnergy Corporation	Disagree	CIP -011-1 Table R5- Physical Security for BES Cyber SystemsItem 5.1: Should specify minimum expectations regarding how physical access should be restricted. There appears to be not difference in the level of security required for Medium and High impact facilities.Item 5.8, 5.9: Why two different revoke authorized unescorted physical access time periods to complete this task? It should be consistent for Control Centers, Generation and Transmission sites to revoke access in one time period to revoke access when no longer required. As stated this is open for confusion and separate corporate polices and procedures for personnel to train, track and manage. If desired to separate time frames it should be based on Low - Medium - High impacts which is not reflected.Additionally, we do not agree with the shortened time frame to revoke access to those who no longer require access -what justifies change? It should remain consistent with current CIP Ver 2 - Certain business processes and day to day operations will cause unrealistic burden in tracking from manual or automated process to revoke

#	Organization	Yes or No	Question 16 Comment
			access for no cause in shortened time frameItem 6.1 Should specify minimum expectations regarding how physical access should be restricted. There appears to be not difference in the level of security required for Medium and High impact facilities.
16.26	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
16.27	Ameren	Disagree	Due to the scope of the number of medium facilities it will be burdensome and labor intensive to maintain documentation of R5.1 physical security controls with no added protection to the BES. Suggest removing Medium Impact Systems from R5.1.
16.28	Entergy	Disagree	Entergy disagrees with the requirements 6.1, 6.2 and 6.3 to restricting, monitoring and maintenance testing to the systems and provide physical access control over Medium BES Cyber Systems when there is no requirement to monitor or log access into a Medium BES Cyber System, again there is a conflict with the requirements for Medium BES Cyber Systems. High BES Cyber Systems access for unescorted access and visitors alike logged and monitored for ingress and egress. If a systems is going to put in place to monitor egress for visitors then the same system could monitor unescorted personnel as well, this would reduced the maintenance of logs for visitors verses unescorted should be into and out unescorted and visitor alike for HIGH BES Systems should have a very high degree of control including the security systems providing access and monitoring.
16.29	Southern Company	Disagree	For 5.1, More specificity is probably called for here. What standard of care is called for? What does “protecting BES Cyber Systems” mean? Does it just mean “containing”?In 5.2, what are the boundaries of “monitoring”? Does this require real-time observation, alarm response, or after-the-fact review? What constitutes monitoring?5.5 “Authorize” should be replaced with “Control” or “Place limits on”.5.9 creates a responsibility for an Entity to monitor the employment status of all of its contracting companies; the requirement should be eliminated, changed to cover employees only, or changed to 72 hours from notification by contracting company.There is a need for greater differentiation based on connectivity and BES component types in R5 and R6. Having

#	Organization	Yes or No	Question 16 Comment
			one set of physical security standards for the differing types of BES components leads to trying to implement standards in an environment to which they are not suited - for example, several of the requirements do not make sense in a substation environment. The tables for R5 and R6 should be reviewed on a per-requirement basis to take these differences into account.
16.30	MRO's NERC Standards Review Subcommittee	Disagree	For item 5.1, we propose making the Low Impact and Medium Impact criteria "Required". Restricting physical access is something that should, and is probably already, being carried out almost everywhere in the BES. Physical security is one of the first lines of defense for all facilities, but the most important defense for those facilities without routable external connectivity.For item 5.2 through 5.11, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability. This approach builds consistency within R5 and R6.Item 5.3 requires entities to "log" access, and item 5.4 requires entities to "log (manual or automated)" access. Either item 5.3 should define the scope of "logging" access, or "manual or automated" should be deleted from item 5.4 because "log" by itself could already indicate either manual or automated processes.For item 5.7, since termination with cause could occur without warning, revoking access within 24 hours may not be practical at distributed locations without routable external connections, where changes may need to be implemented locally. We would propose including a longer timeline for areas without routable external connections. We also believe a two tiered approach would be practical, where personnel specific access devices (manual keys, key cards, etc.) are removed immediately, and then wide scale access changes (shared combination locks, etc.) are allowed more time to be addressed. We believe this approach is similar to that of the NRC.For items 6.1 - 6.3, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard.For items 6.1 - 6.3, the drafting team may want to consider how these requirements apply to areas without any

#	Organization	Yes or No	Question 16 Comment
			type of automated physical access control system. What if access is simply restricted by keys, manual logging, and door alarms transmitted by the local RTU to a Control Center? This approach would appear to meet the requirements of R5, but would not seem to be applicable to the requirements of R6.
16.31	The Empire District Electric Company	Disagree	For item 5.1, we propose making the Low Impact and Medium Impact criteria "Required". Restricting physical access is something that should, and is probably already, being carried out almost everywhere in the BES. Physical security is one of the first lines of defense for all facilities, but the most important defense for those facilities without routable external connectivity.For item 5.2 through 5.11, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability. This approach builds consistency within R5 and R6.Item 5.3 requires entities to "log" access, and item 5.4 requires entities to "log (manual or automated)" access. Either item 5.3 should define the scope of "logging" access, or "manual or automated" should be deleted from item 5.4 because "log" by itself could already indicate either manual or automated processes.For item 5.7, since termination with cause could occur without warning, revoking access within 24 hours may not be practical at distributed locations without routable external connections, where changes may need to be implemented locally. We would propose including a longer timeline for areas without routable external connections.For items 6.1 - 6.3, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard.For items 6.1 - 6.3, the drafting team may want to consider how these requirements apply to areas without any type of physical access control system. What if access is simply restricted by keys, manual logging, and door alarms transmitted by the local RTU to a Control Center? This approach would appear to meet the requirements of R5, but would not seem to be applicable to the requirements of R6.

#	Organization	Yes or No	Question 16 Comment
16.32	BGE	Disagree	General: What is an "area"? With the elimination of PSP this leaves "area" up for debate. Provide definition for "monitor" (is this manual, automated, 24x7??). 5.1 - Remove the requirement for medium impacted systems (currently says "required for external connectivity only, this requirement is pertaining to physical access). Combine 5.3 & 5.4 and reword to say "Log the entry and exit of all individuals with access to an area protecting BES Cyber Systems." 5.8 & 5.9 should not be restricted to removal from Control Center Only. This should be "areas protecting BES Cyber Systems" to maintain consistency. Define "Generation or Transmission Facility". Define "invalid access". To what extent does physical access mean, does it mean dispatching a guard for every single invalid access attempt? Under 5.8 access is revoked for Medium and High impacted systems but in 5.11 there is no requirement to review access for Medium impacted Systems.6.3 Physical access control systems were not defined in 5.1, 5.2 & 5.3. Should read "Implementing a maintenance and testing program for systems used to comply with 5.1, 5.2 & 5.3)." Define "physical security mechanism".
16.33	Constellation Energy Control and Dispatch, LLC	Disagree	-In 5.1 remove the requirement for medium impacted systems, which is not appropriate for a requirement pertaining to physical access.-Eliminate the timing differences for revoking access between Control Centers, generation or transmission facilities and use a single timing requirment for access to all BES cyber systems.
16.34	Bonneville Power Administration	Disagree	In general, Table R5 is acceptable, other than the items discussed below.We understand the impact of FERC requiring immediate revocation. However, it is difficult to see how to achieve that in every case. The standard should be based upon what is achievable and reasonable for both routine revocation and revocation for cause. The table should have a closer resemblance to R9.Section 5.8 and 5.9: 36 or 72 hours seems very short for revoking access for people who, presumably, are still trustworthy, but merely no longer need access or who have left the entity under routine circumstances. They simply no longer require access because of a job change. Such revocation should be a routine, normal business-day action. 72 hours does not allow for business-day action during a long weekend. In fact, for a large organization revocation for field assets in such a short

#	Organization	Yes or No	Question 16 Comment
			time period would often be impossible. Recommend changing this to five business days or five calendar days. We also recommend using the same criteria for all assets: Control Center, generation, or Transmission Facility.Section 5.11 is very good: it makes it clear that unauthorized access is an incident, not a violation.Table R6, 6.1-6.3 require the plans to address Part 5.1-5.3 if identified as "Medium". However, 5.2 and 5.3 do not require physical security under "Medium". How can a plan address elements that are not required?
16.35	Idaho Power Company	Disagree	In R5, if access authorization is not required for medium impact systems then why is there a requirement to revoke authorized access if it was never authorized in the first place.
16.36	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
16.37	Southern California Edison Company	Disagree	Local logical (electronic) access is and should be recognized as a type of role based access where one has to be physically present, near a device, to operate it. The boundary protection for this type of role is: (1) the physical security boundary; and (2) the device level electronic security boundary. The proposed standard as it is currently worded allows for the removal of at least one access mechanism at the time of revocation. In that case, removal of access through the physical boundary will ensure the immediate revocation of a component critical for this type of role. The drafting team should add additional revocation criteria to adequately address this type of revocation.While this control is easily implemented in a control center or data center environment, field devices that are often located over vast geographic areas pose compliance challenges. This requirement may result in the creation of substantial organization capabilities for compliance without a comparable improvement in reliability of the BES. SCE believes Requirement 5.1 should apply to low impact BES Cyber Systems and Requirement 5.5 should apply across all impact levels. For many field devices, where enforcement of cyber security controls in a timely fashion may be a challenge given the large geographic operational areas, limitation of physical access may be the most

#	Organization	Yes or No	Question 16 Comment
			effective control. Limiting unrestricted access, even to Low impact devices and the ability to control such access, could be a mitigating factor for the inability to perform device by device access revocation where no external access exists.
16.38	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.Table R6 Row 6.3, it is appropriate to validate those basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.39	Oncor Electric Delivery LLC	Disagree	Physical security should only be required at control centers and High impact substations with IP based communications.
16.40	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation 'Required for external connectivity only' in R5.1. This is an odd mix of physical and electronic access requirements. Please define the stipulations 'Required for external connectivity only' in R6.1, 6.2 and 6.3 for the same reasons.
16.41	WECC	Disagree	Recieved a uniform disagree from all but a vast range of responses to this question depending on the function of the entity reviewin the question.Low levels seem inappropriate as there is veryminimal requiremens for security based on the current tables.andShould apply to all impact levels.
16.42	Hydro One	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements

#	Organization	Yes or No	Question 16 Comment
			5.5, 5.6, 5.7 and 5.11 should have a specification for BES Medium Impact Cyber System.Please clarify Requirements 6.1, 6.2 and 6.3. Is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.43	ISO New England Inc	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements 5.5, 5.6, 5.7 and 5.11 should specify something for BES Medium Impact Cyber System.Request clarification on Requirements 6.1, 6.2 and 6.3 is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.44	Northeast Power Coordinating Council	Disagree	Recommend that revising unescorted physical access depends on BES Impact. Requirement 5.8 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirement 5.9. For consistency with Requirement 5.1, Requirements 5.5, 5.6, 5.7 and 5.11 should have a specification for BES Medium Impact Cyber System.Request clarification for Requirements 6.1, 6.2 and 6.3. Is the routable connectivity on the BES Cyber System or the physical access control system?Should the "routable connectivity" be "external connectivity" for Requirements 6.1, 6.2 and 6.3?
16.45	ReliabilityFirst Staff	Disagree	ReliabilityFirst believes the existing defined term "Physical Security Perimeter" should be retained and used in CIP-011. The current proposed language, "Restrict Physical access to areas protecting BES Cyber Systems", could lead to many questions for an auditor. Further, we believe that all rows of Table R5 (5.1 through 5.11) should be "required" for Medium Impact BES Cyber Systems. For Table R5, row 5.11; what constitutes an unauthorized physical access attempt? If unintended triggering of a magnetic card reader (such as simply walking too close to a reader and unintentionally activating it) indicates "failed attempts", are those to be considered unauthorized access attempts? Also in row 5.11, within what time frame must the review be conducted and we believe

#	Organization	Yes or No	Question 16 Comment
			there should be a requirement to document the review.
16.46	Luminant	Disagree	Remove the requirements for Medium Impact systems
16.47	Nuclear Energy Institute	Disagree	Requirement R6, Medium Impact: allowances should be included to exclude BES cyber systems which incorporate one way connectivity (e.g. outside the ESP via a one way hardware device), even if the protocol is routable. This would be in addition to the existing non-routable protocols.
16.48	Exelon Corporation	Disagree	Requirements 5.8 and 5.9 contain time parameters in hours. Exelon's tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required, it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time levels and having a different timeframe for a control center than other locations? It is difficult to understand how the impact levels were determined. The basis of the original CIP Standards addressed the critical sites and took into account the nature of the Critical Cyber Assets that could impact the BES, not the functional/operational parameters of the equipment that is connected to the BES. Exelon's position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.We are also concerned about the practicality of potentially applying these standards to multiple unmanned locations. Items 5.1, 5.2, 5.3: Requiring this level of physical security for any BES Cyber System that has no external connectivity should be reconsidered. No matter what level of impact, entities should not have to provide more physical security for a cyber based device or protective relay when it has no external connectivity and therefore would have no more impact to the BES than the other electromechanical devices, protective relays or control switches mounted in the same control panel.

#	Organization	Yes or No	Question 16 Comment
16.49	Progress Energy - Nuclear Generation	Disagree	See attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
16.50	Xcel Energy	Disagree	See comments on question 15
16.51	Western Area Power Administration	Disagree	See previous comments
16.52	Emerson Process Management	Disagree	Since physical access restriction is not required for low and, maybe, medium impact BES Cyber Systems, according to R2 and R3, everyone in a generation plant will be subject to awareness and training requirements. Further, per R3.1, the training will cover the proper use of BES Cyber Systems, the proper handling of BES Cyber Systems information and storage media, and others. Why do plant's administrative staffs need to know how to use BES Cyber System?
16.53	Detroit Edison	Disagree	Table entries 5.8 and 5.9 require access revocation for Medium Impact access that is not required to be explicitly authorized.Table entries 5.8 and 5.9 should address the concept of expired PRA and/or training requirements. Propose changing 5.8 and 5.9 to read:"...who no longer require such access or no longer meet the training or PRA requirements as specified in R3 or R4..."Table entries 6.1, 6.2, and 6.3 Medium Impact states "Required for routable connectivity only". This term is not defined. We suggest replacing that language with "BES Cyber Systems that use a routable protocol".
16.54	EEI	Disagree	Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a particular item or location.Table R5 Row 5.9 creates a responsibility for an Entity to monitor the employment status of all of its contracting companies; the requirement should be eliminated, changed to cover

#	Organization	Yes or No	Question 16 Comment
			employees only, or changed to 72 hours from notification by contracting company.In general, there is a need for greater differentiation based on connectivity and BES component types in R5 and R6. Having one set of physical security standards for the differing types of BES components leads to trying to implement standards in an environment to which they are not suited - for example, several of the requirements do not make sense in a substation environment. The tables for R5 and R6 should be reviewed on a per-requirement basis to take these differences into account.
16.55	Allegheny Energy Supply	Disagree	Table R5 Row 5.3: This requirement should be consistent with Row 5.4 with respect to logging entry and exit.Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.56	Allegheny Power	Disagree	Table R5 Row 5.3: This requirement should be consistent with Row 5.4 with respect to logging entry and exit.Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.57	American Electric Power	Disagree	Table R5:5.1, Column "Medium Impact BES Cyber System", regarding "Required for external connectivity only", this should be stated "routable external connectivity"?5.8 & 5.9, Column "Medium Impact BES Cyber System", regarding "Control Center only" and "generation or Transmission Facility only". Authorized unescorted physical access is not required for medium impact facilities in row 5.5. If it is not required in 5.5, how can it be revoked in 5.8?5.11, regarding "...unauthorized physical access attempts". Suggested wording: "unauthorized physical access or physical access attempts".Table R6:6.1: Row 5.1 only requires access to areas protecting BES Cyber Systems be protected. It does not say that it needs to be done with a control system. A pad lock can used to restrict physical access. It also requires it for any external connectivity, not just routable.6.2: Monitoring of Medium Impact BES Cyber Systems is not required in section 5.26.3: A physical security control system is not needed to meet row 5.1 on Medium impact

#	Organization	Yes or No	Question 16 Comment
			Facilities since no other requirements from Table 5 are needed.
16.58	Alberta Electric System Operator	Disagree	Tables R5 and R6 do not log, monitor, or control physical security and access to Low Impact BES Cyber Systems. Consider making the requirements in tables R5 and R6 more restrictive. For example, restrict physical access for all impact levels, but make frequency and time horizon of reviews dependent on impact level - Low Impact review semi-annually, Medium Impact quarterly, and High Impact monthly.In table 5.4 - Change to "Log (manual or automated) visitor access (individuals not authorized..." to be consistent with Table 5.3.
16.59	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS proposal to include the Low and Medium Impact requirement in 5.1, but as stated in our response to Question 14, we believe the implementation of this requirement must be for a reasonable physical access policy, for example, as required for employee and public safety code compliance. Compliance with this requirement should be straight forward: locked gates, locked control house doors and/or locked fence around BES Cyber systems. Table R5 Item 5.1 should state for Low and Medium Impact; "Required".The APPA Task Force supports the MRO-NSRS proposal For items 5.2 through 5.6; we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We also suggest the following language for the tables noted:R5 Table 5.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR5 Table 5.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.4: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.5: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR5 Table 5.6: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredThe APPA Task Force recommends removal of Table Items 5.7 - 5.9, dealing with "revoking authorized unescorted access," since this is covered in Table 9.2-9.5, Access Revocation. We believe there should not be a distinction between the two revocations and the timeframes for the revocation should be the same. There

#	Organization	Yes or No	Question 16 Comment
			should be only one set of revocation requirements.R5 Table 5.10: (renumber if 5.7-5.9 are removed)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR5 Table 5.11: (renumber if 5.7-5.9 are removed)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredThe APPA Task Force supports the MRO-NSRS proposal for items 6.1 - 6.3; hence, we would propose all Medium Impact criteria to be changed to "Required for routable external connectivity only", to maintain consistency with existing wording within the standard. The tables would then read:R6 Table 6.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR6 Table 6.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR6 Table 6.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredThe APPA Task Force believes the 3 year maintenance and testing requirement on "all physical security mechanisms" in 6.3 is unreasonable. The term "all" should be replaced with "major" and the timeframe should be based on manufacturer recommendations, not an arbitrary 3 year timeframe.
16.60	Black Hills Corporation	Disagree	The concept makes sense, but 5.2 & 5.3, and 6.2 & 6.3 should have consistent impact applicability.
16.61	Network & Security Technologies Inc	Disagree	There are a number of inconsistencies in these and other tables related to grant and revocation of access (e.g., 5.1 requires restriction of physical access to areas protecting Medium Impact systems with external connectivity but 5.5 does not indicate such access must be authorized). Recommend a complete "scrub" of all requirements pertaining to authorization of, control of, and revocation of physical and electronic access.
16.62	We Energies	Disagree	We Energies agrees with EEI comment: Table R5 Row 5.1 needs to document basic physical security requirements for all low and medium BES Cyber Systems.We Energies agrees with EEI comment: Table R5 Row 5.2: There should be additional language describing what "Monitoring" means. Does Monitoring mean 100% guarantee of any alert or alarm that would indicate an attempt or actual breach in physical security? We Energies agrees with EEI: Suggested language: Monitoring means: The act of conducting a systematic and repeated sequence of measurements, or observations, to assess a

#	Organization	Yes or No	Question 16 Comment
			particular item or location.We Energies agrees with EEI comment: Regarding Table 6, it is unclear what the benefit is for having requirement differentiation for Medium BES Cyber Systems with routable connectivity vs. those without.We Energies agrees with EEI comment: Table R6 Row 6.3, it is appropriate to validate that basic controls, e.g. a padlock or substation fence protecting a low Impact BES Cyber System are tested and maintained periodically.
16.63	Progress Energy (non-Nuclear)	Disagree	Why does Table R6 require access control to systems identified in 5.1, 5.2, 5.3 medium impact with routable connectivity, but 5.1 does not reference routable and 5.2, 5.3 have no requirements for medium impact?See comment 14.

17. Requirement R7 of draft CIP-011-1 states "Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 – Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of electronic access control requirements that are included in Requirements table R7? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please Explain and provide any suggestions for modification.

Summary Consideration:

Comments concerning the requirement language in Requirement R7 with regard to "acceptable use" and the requests for clarity of the term "account types" indicated that these terms were misunderstood. The term "acceptable use" has been replaced with a requirement to authorize the use of account types, and the associated guidance document has been expanded to include descriptions of account types as used in this requirement.

Many commenters indicated that the format of Requirement R7 was causing confusion, suggesting that consistency in the use of columns and the format of the requirements and other information included in the tables would be helpful. The SDT agreed, and made consistency changes in the format and content of the columns in the tables, including the information required for High, Medium, and Low Impact BES Cyber Systems and BES Cyber Assets.

#	Organization	Yes or No	Question 17 Comment
17.1	ERCOT ISO	Agree	7.1: Please clarify "identification" and "group account".
17.2	Duke Energy	Agree	It's unclear how R7 tasks accomplish the purpose statement for low impact systems.
17.3	Minnesota Power	Agree	Minnesota Power generally agrees with the list of electronic access control requirements included in Table R7. However, it believes that some confusion exists regarding what distinguishes a "group" account from a "shared" account or a "system" account from an "administrative" account as described in Part 7.1.In addition, many types of equipment found in generating facilities or substations do not have typical "accounts," although they may have some type of access control (i.e., configuration password). To add further clarity, Minnesota Power recommends that the following be added to the end of purpose statement for Requirement 7:"...Required for only BES Cyber System

#	Organization	Yes or No	Question 17 Comment
			Components with account management capabilities."
17.4	Puget Sound Energy	Agree	Puget Sound Energy suggests that, because a BES Cyber System is made up of multiple components (hardware, operating system, application) that there should be a little clarity added. For example: "Identification of account types...and administrative accounts, in use for the BES Cyber Systems at the operating system, and applicable application(s) on the BES Cyber System Components."
17.5	Progress Energy - Nuclear Generation	Agree	R7 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
17.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 6.
17.7	Bonneville Power Administration	Agree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.
17.8	Entergy	Agree	This matches the guidance presented in the nuclear industry document NEI-08-09 Rev 6 Section 1.2.
17.9	Green Country Energy	Agree	Would it be possible throughout the standard to footnote sources for guidance such as DHS catalog of control systems or specific NIST documents? Hopefully this would remove some of the ambiguity and lead towards a more results based standard.

#	Organization	Yes or No	Question 17 Comment
17.10	Independent Electricity System Operator	Disagree	- Should R7.1 include anonymous to be consistent with R8.3.- R7.2 appears to be a policy statement vs something that can be audited. Some violations of acceptable use can't be detected or monitored so how can this be audited? If this is a policy stateme
17.11	Southwest Power Pool Regional Entity	Disagree	7.1 needs to include both local and domain user accounts. Elaborate a bit more on what is meant by "group" account. In many cases, a group account and a shared account are the same account. Very easy to overlook the group categorization the way the requirement is written as it is not defined in the current CIP standards.
17.12	US Army Corps of Engineers, Omaha Distirc	Disagree	7.2 implies that the user agreements would be so detailed as to differentiate the valid uses of individual systems and account types. It should be possible to have user agreements that allow them to work on authorized systems for authorized purposes (ie sysadmin account is authorized for sysadmin work) and restrict use for unlawful and non business purposes.
17.13	BCTC	Disagree	Please provide a definition of Acceptable Use. It is recommended that the term "acceptable use" be replaced (i.e. are we looking to define the roles within the BES Cyber System and define what actions each can take within the system?)
17.14	Idaho Power Company	Disagree	Acceptable use is a broad term when it comes to administrative accounts. As long as acceptable use can be defined in general terms and does not require a definitive list, this requirement will be OK. If it requires a definitive list, then there is risk in trying to define every situation or use of an administrative account.
17.15	Constellation Energy Control and Dispatch, LLC	Disagree	Account types should be defined.
17.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.

#	Organization	Yes or No	Question 17 Comment
17.17	The Empire District Electric Company	Disagree	Comments: Many types of equipment found in generating facilities or substations do not have typical “accounts”, although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: “Required for only BES Cyber System Components with account management capabilities.”
17.18	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes a technical feasibility exception may be required based on the current wording of this requirement when considering local access to programmable electronic devices in a substation environment that do not support the ability to demonstrate acceptable use. Also for R7.2, CenterPoint Energy is not sure what is meant by "Acceptable use of each identified account types" and suggests adding specific examples.
17.19	Kansas City Power & Light	Disagree	Do all cyber systems and component that may be identified here have the capability to have an account? Recommend consideration of additional language such as “where equipment capabilities allow” for R7.
17.20	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Documentation requirements would be burdensome without preventing malicious activity.
17.21	Dominion Resources Services, Inc.	Disagree	Dominion presumes that the word “acceptable” used in 7.2 will be defined by the Reliability Entity and will not be dictated by an outside group.
17.22	E.ON U.S.	Disagree	E.ON U.S, does not believe a compliance requirement is necessary for the low impact category.
17.23	Western Area Power Administration	Disagree	How is the responsible entity to meet this requirement for BES Cyber system components that do not have specific account types? For example...relays, comm equipment, other substation equipment that may now be part of the “affect situational

#	Organization	Yes or No	Question 17 Comment
			awareness of the BES" portion of the requirement.
17.24	Matrikon Inc.	Disagree	I would separate the requirements of creating an "inventory of user accounts" and its application to BES Cyber Systems, from the requirement of assigning "ownership and authorization of user accounts".The key separation is the "inventory" and the "authorization/use" of those accounts. A Cyber system may have 5 user accounts, of which some are disabled, some are shared, and some are actively used by specific individuals.
17.25	Florida Municipal Power Agency	Disagree	Is R7 needed since the real reliability goal is accomplished in R8? "Shall document" is not a strong requirement. The requirement is really account management. FMPA suggests: "Each Responsible Entity shall manage accounts and account permissions in the manner described in CIP-011-1 Table R7 - Account Management Specifications".Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, if R7 is kept, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
17.27	American Transmission Company	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities."
17.28	MidAmerican Energy Company	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration

#	Organization	Yes or No	Question 17 Comment
			password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.29	MRO's NERC Standards Review Subcommittee	Disagree	Many types of equipment found in generating facilities or substations do not have typical "accounts", although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: "Required for only BES Cyber System Components with account management capabilities." Without this addition, we believe this item sets the stage for numerous TFE's within the industry.
17.30	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement 7.1 within table 7 should provide guidance to identify role based access controls for accounts on the BES Cyber System components. The current way the requirement reads, it is unclear if the specific account types listed are the only ones required for identification. Additionally, the BES Cyber Systems may not have the specific account types listed in requirement 7.1. Furthermore, NextEra believes requirement 7.2 should provide additional guidance related to acceptable use. It is unclear if the acceptable use requirement should be defined per account on each BES Cyber System Component. The requirement should require acceptable use based on role based access controls for categories of accounts. What is the criteria for 7.2 "Acceptable use" of each identified account types? Please add a local definition of "acceptable use" within the standard.Regarding R7, this table seems to apply the CIP electronic account standards to all units. Is this the intent?If so, then for 7.1 - the volume of research and account management, we suggest applying this to high impact only.As for R11.1 does the user restriction for wireless technologies include Blackberries and SmartPhones, NextEra believes this would impact on volume of devices and would be burdensome to manage.NextEra would like to see statement treating personal communication devices the same as company issued laptops since there are internal access controls designed to prevent misuse.

#	Organization	Yes or No	Question 17 Comment
17.31	Indeck Energy Services, Inc	Disagree	Not all Cyber Systems have logins and accounts. [suggestion] “For any Cyber System permitting login access, each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 - Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.”
17.32	Network & Security Technologies Inc	Disagree	Purpose of R7.1 is unclear. Is it intended to require that every type of account a given individual has authorization to use be identified? If so, please clarify.Suggest “acceptable use” be addressed in R1 (policy) rather than here.
17.33	LCEC	Disagree	R7 - “access to its BES Cyber Systems “ should read “Access to a BES Cyber System or its components “Roles should be identified during the creation of accounts.R8 - R7 and R8 should be combined into managing accounts.In CIP 10 there should be an air-gap exclusion for the thousands of relays connected to medium impact or lower systems that would require access revocation.
17.34	Consultant	Disagree	R7 - The wording to implement the criteria in the tables is incorrect. The tables are specifying the requirements and application of requirements to the classes of assets resulting from the impact categorization process. The wording of the statement should be modified to reflect this distinction.R7 & Table: In this section there is a change in terminology from the requirement to the table name to the column heading for the requirements. For this requirement:R7: document BES Cyber System accountsTable Name: Account Management Specificationscolumn Heading: Account Management DocumentationThis is confusing, as it is not clear what the topic is being addressed. Suggest consistent terminology for these locations. NOTE: There are multiple requirements where this condition exists and should be addressed.R7 - Account management would not seem to prevent malicious operation of BES Elements. It would seem to maintain control of access to BES Cyber Systems. The grouping of Electronic Access Controls would be more likely to be used to prevent malicious operation. R7 - Suggest deleting the word "maintaining" as account management controls access to BES

#	Organization	Yes or No	Question 17 Comment
			Cuber Systems, and the word maintaining control is unnecessary.7.1 Suggested rewording: For each BES Cyber System identify the account types in use on that system, including individual, group, shared, system, and administrative accounts.7.2 The intent is not clear. Does this mean document the acceptable use of each account type on each system, or document the acceptable use of the account types in use across all BES Cyber Systems? The resulting documentation is significantly different.
17.35	Southern Company	Disagree	R7 creates a workload requirement with very little benefit to overall reliability.
17.36	SCE&G	Disagree	R7 Is every BES Cyber Sytem required to have account types. Will there be provisions for equipment incapable of having an "account type"?R9 When does the timetable start for personnel terminated for cause? Once paperwork is completed?R10 SDT should consider the high volume of TFEs that may be generated for equipment with hardcoded passwords that cannot be changed. The TFE process should be evaluated and revised to make it less burdomesome on entities to document that a password is incapable of being changed every 12 months, or a provision should be added to the requirments. Overall provisions should be added to allow entities to utilize more secure methods of account access control, such as RSA tokens, without burdening the entity with additional adminsitrative work for choosing an access control method which is inherently more secure.R11: The box containing the definition for remote access: is this remote 2-way or 1-way?
17.37	Luminant	Disagree	R7.1 should not be required for low impact.
17.38	ISO New England Inc	Disagree	R7.2 appears to be a policy statement vs something that can be audited. Some violations of acceptable use can't be detected or monitored so how can this be audited? If this is a policy statement then it should be relocated to R1.
17.39	Ameren	Disagree	R7.2 does not list a monitoring frequency, it implies continual monitoring. Recommend that a monitoring frequency be added to this requirement.

#	Organization	Yes or No	Question 17 Comment
17.40	Powersouth Energy Cooperative	Disagree	R7-14. The required electronic security measures should be limited to the access or gateway point. Strong security measures at the gateway can effectively protect all the cyber assets that are accessed through the gateway. An argument can be made for example that the frequent changing of passwords on tens if not hundreds of devices inside a boundary that has very strong security measures lessens reliability should a qualified employee need to access the device but not be able to do so due to a recently changed password. Little is gained by requiring hundreds of devices inside a secure boundary to have the same level of protection that is provided through a secure gateway. Just because "it can be done" does not mean that "it should or must be done". The objective is to protect the assets. It should be recognized that protecting the assets can be done by focusing on the gateway that allows access to the devices. This allows entities to keenly focus on managing the security of those points of access rather than spending time, capital and other resources that provide limited if any added security. Prior to the workshop it was felt that strong gateway protection would meet the objectives of the standard. However, that is no longer clear. For example, it was felt that at a substation strong security measures at the gateway that allowed access to the cyber devices would meet the objective of standard with the cyber system (a collection of protective relays or other devices) being protected by the secure gateway. It appears that may not be the case. This results, for example, in the failure to change a password in a single device on a secured network being non-complaint with the standard for a situation where the BES reliability was never jeopardized. That type approach will likely result in numerous non-compliances that will on serve wasted resources even though the BES was never jeopardized. If it is intended that protecting only the gateway meets the objective that needs to be made clear.
17.41	BGE	Disagree	Replace the word "element" with "Cyber System Component" to maintain consistency with the defined terms. What is the difference between group and shared? What is the definition of "Acceptable use"?
17.42	San Diego Gas and Electric	Disagree	SDG&E recommends separating Wireless concepts from Access Concepts. Wireless is a

#	Organization	Yes or No	Question 17 Comment
	Co.		method of access, as is VPN, Citrix, dial-up, etc..., while Access implies a physical and logical service provided to a client.
17.43	Garland Power and Light	Disagree	Shared & group accounts should not be created or allowed because there is no accountability for these accounts
17.44	APPA Task Force	Disagree	The APPA Task Force does not believe the description of R7 follows the intent of the requirement. The following are recommended edits:R7. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems.R7. Requirement:Each Responsible Entity shall document manage BES Cyber System accounts Components with account management capabilities by incorporating the criteria specified in CIP-011-1 Table R7- Account Management Specifications R8. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems. R8. Requirement: Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 - Account Management Implementation R9. Objective: To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems. R9. Requirement: Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 - Access Revocation R10. Objective: To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber SystemsR10. Requirement:Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 - Account Access Control Specifications The drafting team uses the word "any" in the description in R11 and R12. This appears to require the all BES Cyber Systems be included in the requirement, even if the wireless functionality is disabled. The APPA Task Force believes the description should read: R11. Objective:To ensure that only authorized access is allowed to BES Cyber Systems that have remote or wireless electronic access.R11. Requirement: Each Responsible Entity that allows remote or wireless electronic access to a BES Cyber System shall apply the criteria specified in CIP-011-1 Table R11- Wireless and Remote Electronic Access Documentation for that specific BES Cyber System R12. Objective:To ensure that only authorized access is allowed to BES

#	Organization	Yes or No	Question 17 Comment
			Cyber Systems that have remote or wireless electronic access.R12. Requirement:Each Responsible Entity that allows wireless and remote electronic access to a BES Cyber System shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 - Wireless and Remote Electronic Access Management for that specific BES Cyber System. R13. Objective:To prevent malicious operation of BES Elements by maintaining control of access to the Responsible Entity's BES Cyber Systems.R13. Requirement:Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems [it owns and operates?] by implementing the criteria specified in CIP-011-1 Table R13 - Remote Access Revocation R14. Objective:To ensure that only authorized access is allowed to BES Cyber Systems that have remote or wireless electronic access.R14. Requirement:Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to the BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 - Wireless and Remote Electronic Access Controls.
17.45	Southern California Edison Company	Disagree	The drafting team should clarify mapping of controls, as identified in CIP-005 R1.5, and unbundle these requirements for access control devices. This would be in agreement with the drafting team's stated objective to leverage the financial and organizational capital invested by registered entities in providing cyber security through compliance with current versions of the CIP standards. SCE believes that all instances of electronic access, whether to the boundary or a system/device within the boundary, should be in one requirement. A new standard for access may include these account related controls in addition to others.The drafting team should provide guidance for R7.2. As written, R7.2 suggests that the acceptable use for each identified account type is required across all impact levels. It is not clear whether the intent here is to document business justification(s) for the acceptable use, the posting of signage describing acceptable use, or both. SCE recommends that the drafting team explicitly state the intent of this requirement.

#	Organization	Yes or No	Question 17 Comment
17.46	US Bureau of Reclamation	Disagree	The use of terminology is a problem in this standard. It is suggested that the term "electronic access" should be used instead of the term "account";or, a definition should be developed to clearly differentiate the difference, if there is one. The term electronic access is more precise.
17.47	Public Service Enterprise Group companies	Disagree	This is too short a period, especially if the event occurs over a weekend or holiday. The timeframe should be changed to 5 calendar days or 3 business days. At a minimum, 72 hours.
17.48	Pepco Holdings, Inc. - Affiliates	Disagree	What is a Cyber System account? Does this exclude Cyber System Component accounts? Would microprocessor relays passwords be in scope? Please reference comments on BES Cyber System Components and BES Cyber System definitions.
17.49	Manitoba Hydro	Disagree	What is the definition of “Acceptable use” for Requirement R7.1?

18. Table R7 provides direction concerning what impact level of BES Cyber Systems to which Requirement R7 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011 R7 was moved to CIP-007-5 R5.

Several commenters expressed concern that the documentation requirements for Low Impact BES Cyber Systems would be burdensome and would not prevent malicious activity. In response, most documentation and technical requirements applying to Low Impact BES Cyber Systems have been removed. However, the requirement for changing the default password remains, because this addresses a significant vulnerability and does not require periodic maintenance.

Some commenters suggested the standards need to be more explicit as to whether the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components. In response, the SDT provided additional clarity as to when a requirement applies to individual Cyber Assets. However, the requirements are written to allow flexibility in implementation.

In addition, commenters suggested adding "Required for routable connectivity only" to the applicability for Low and Medium Impact BES Cyber Systems. In response, the applicability for this requirement has been modified to High and Medium Impact BES Cyber Systems. For Medium Impact BES Cyber Systems, the SDT does not believe that the communication attributes of the BES Cyber System adequately mitigate the vulnerability this requirement addresses.

#	Organization	Yes or No	Question 18 Comment
18.1	Idaho Power Company	Agree	Account types will not vary by BES impact.
18.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
18.3	The Empire District Electric Company	Agree	Comments: We agree, assuming the suggested statement under question 17 is included.
18.4	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.

#	Organization	Yes or No	Question 18 Comment
18.5	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comments for question 6.
18.6	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels of R7 if the drafting team accepts our edits proposed in response to question 17.
18.7	Duke Energy	Agree	This is a lot of work to do for low impact systems. We suggest the requirement be removed from R7. Please provide insight as to how these tasks accomplish the purpose for low impact systems.
18.8	MRO's NERC Standards Review Subcommittee	Agree	We agree, assuming the suggested statement under question 17 is included.
18.9	BGE	Disagree	7.1 and 7.2 remove the requirement for low and medium since we do not need to log and monitor those systems per R8.
18.10	The United Illuminating Co	Disagree	7.1 and 7.2 should not apply to Low Impact devices.
18.11	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
18.12	LCEC	Disagree	Clarify if 7.1 & 7.2 are for account types only or if this includes specific accounts.
18.13	Indeck Energy Services, Inc	Disagree	Cyber Systems without login access need to be excluded.
18.14	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Documentation requirements would be particularly burdensome for low impact BES cyber systems.

#	Organization	Yes or No	Question 18 Comment
18.15	E.ON U.S.	Disagree	E.ON U.S, does not believe a compliance requirement is necessary for the low impact category.
18.16	Minnesota Power	Disagree	It appears inconsistent with the other Requirements of CIP-011-1 to apply the criteria specified in Parts 7.1 and 7.2 to Low Impact BES Cyber Systems. If those using accounts on Low Impact Systems are not required to have Training, as required in R3, how are they to know the acceptable use of these accounts and therefore, why inventory and document it?
18.17	LADWP	Disagree	Low impact BES Cyber Systems should not be required.
18.18	National Grid	Disagree	National Grid suggests removing controls for Low Impact BES CS in table R8 to be consistent with table R7.7.2 - Elaborate on “acceptable use” and documentation required for acceptable use
18.19	NextEra Energy Corporate Compliance	Disagree	NextEra believes the requirement to identify and document acceptable use of accounts on Low Impact BES Cyber systems should not be required. The exercise of complying to that requirement for Low Impact BES Cyber systems will take considerable effort but will provide little if any security value or improve the reliability or security of the BES Infrastructure. It is recommended to have the requirement apply to both Medium and High Impact BES Cyber Systems.
18.20	American Municipal Power	Disagree	Please provide a little or no impact category.
18.21	Hydro One	Disagree	Presently, R7.1 specifies identification of account types. We suggest that the requirement R7.1 is modified to delete the word “types”.
18.22	Puget Sound Energy	Disagree	Puget Sound Energy notes that physical security measures are only applicable to High Impact and some Medium Impact BES Cyber Systems. Puget Sound Energy suggests aligning Table 7 to Tables 5 and 6, or clarifying “Required for routable connectivity only”

#	Organization	Yes or No	Question 18 Comment
			for Low and Medium Impact BES Cyber Systems. At the very least, Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management.
18.23	Progress Energy (non-Nuclear)	Disagree	R7.1 - account management for "low" assets may be significant when you consider all of the intelligent programmable field instrumentation they will likely be categorized this way.Acceptable use is too broad a requirement. If someone is deemed competent to have access this requirement is not needed.Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.24	Constellation Energy Control and Dispatch, LLC	Disagree	Remove Required status for low and medium BES Cyber Systems, since R8 does not require logging or monitoring of those systems.
18.25	Garland Power and Light	Disagree	Requirement 7.1 & 7.2 should not be required for Low Impact BES Cyber Systems
18.26	Network & Security Technologies Inc	Disagree	See response to 17, previous.
18.27	Constellation Energy Commodities Group Inc.	Disagree	Should not be required for low impact systems.
18.28	Ameren	Disagree	Suggest removing R7.1 and R7.2 for Low Impact Systems. Creating and maintaining recordkeeping for all BES Systems will be a massive undertaking with no added protection to the BES.
18.29	Entergy	Disagree	The requirements should apply across the board for sites where routable protocols and dial-up communications are employed.

#	Organization	Yes or No	Question 18 Comment
18.30	Allegheny Energy Supply	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.31	Allegheny Power	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.32	EEI	Disagree	Use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.33	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments. Please also reference comments on BES Cyber System Components and BES Cyber System definitions.
18.34	American Transmission Company	Disagree	We agree, assuming the suggested statement under question 17 is included.
18.35	We Energies	Disagree	We Energies agrees with EEI use of 'BES Cyber System' vs. 'BES Cyber System Component' - Some requirements (e.g., R7.1 - identification of account type; R16.1 - security patches) use the term 'BES Cyber System', while others use the term 'BES Cyber System Component' (e.g., R23.1 - inventory of the BES Cyber System Component). SDT

#	Organization	Yes or No	Question 18 Comment
			needs to be specific when the requirement applies at the BES Cyber System level or to the individual BES Cyber System Components.
18.36	FirstEnergy Corporation	Disagree	We feel there could be limited value in maintaining account type information for low impact BES Cyber Systems. Suggest removing 'required' for that column of table for R7.
18.37	Manitoba Hydro	Disagree	What is the purpose of Requirement 7.1 for Low Impact BES Cyber Systems? It is not clear that this information is needed for other requirements. Requirement 7.2 is inconsistent with Requirement R3, where no training is required for Low and Medium Impact BES Cyber Systems. Defining acceptable use of account types serves no purpose if it is not provided in training. The meaning of the references in Requirement R7.1 to "account types" and in Requirement R10.8 to "non-privileged accounts" is unclear. The reference in Requirement R7.2 to "Acceptable use of each identified account types" is incomplete. What is it that the Responsible Entity is required to do - develop criteria related to acceptable use, monitor for compliance with such criteria, etc? There are no specifics given with respect to "restrictions" in Requirement R11.1 or "allowed methods" in Requirement R11.2 1, so it is assumed to be at the Responsible Entity's discretion. It is unclear whether Requirement R11.3 requires a written policy to be in place - one would assume no written policy was required by the opening language of Requirement R11.

19. At the present time, the Access Control requirements for Physical Access have not been combined with the Access Control requirements related to Electronic Access. Do you agree with this method? Or would you prefer to have the Physical Access control requirements combined with the Electronic Access control requirements? Please explain and provide any suggestions for modification.

Summary Consideration:

Some commenters expressed concern that physical and electronic access controls may use the same terms, but they can actually mean different things, so there is a need to keep the requirements separate. In response, the terms physical and electric access control have been kept separate, but the controls for authorization, review, and revocation have been combined to ensure consistency across the requirements.

Some commenters expressed the need to combine requirements so that all "revoke" requirements are in one place. The SDT agrees with this suggestion, and the requirements to revoke access have been combined.

Some commenters expressed the need to combine the physical and electronic access control requirements based on the concern that being in separate requirements might lead to an entity missing something. The SDT agrees with this suggestion. The terms physical and electric access control have been kept separate, but the controls for authorization, review, and revocation have been combined to ensure consistency across the requirements.

Some commenters suggested continuing the use of ESP and PSP terminology, since it is now well understood. Upon further review, the SDT decided to continue use of the term Electronic Security Perimeter (ESP), but PSP has been modified to Defined Physical Boundary (DPB) to focus the requirements on controlling access rather than creating a perimeter.

#	Organization	Yes or No	Question 19 Comment
19.1	Duke Energy	Agree with proposed method	Access control for physical and electronic should continue to be separate.
19.2	Dairyland Power Cooperative	Agree with proposed method	Access to a physical area is different than access to an account that provides access to system(s) or application(s). Separate handling is appropriate.

#	Organization	Yes or No	Question 19 Comment
19.3	City Utilities of Springfield, Missouri	Agree with proposed method	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
19.4	Platte River Power Authority	Agree with proposed method	Electronic security and physical security are different disciplines and should be kept separate.
19.5	LCEC	Agree with proposed method	I agree that these should be separate but think that the retired terminology like Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP) are well understood and should not be retired for the sake of change. A lower level of controls does not make sense for physical access in some areas like data centers or control centers but may make sense in areas like substations.
19.6	Southwest Power Pool Regional Entity	Agree with proposed method	Physical access control includes certain requirements, such as escort, that are not applicable to electronic access. If combined, the standard will need to carefully make the appropriate distinction between physical and electronic access controls as necessary.
19.7	Bonneville Power Administration	Agree with proposed method	Physical and Electronic access controls may sometimes use the same terminology, and appear similar, but they are very different disciplines. Physical security may use electronic tools are part of its tool kit. However, it is still primarily a physical and geographical control methodology. Electronic access controls are more amorphous, with boundaries being at once more difficult to define, but more easily and absolutely controlled. Combining them would only lead to confusion and probably to failure in the end.
19.8	FirstEnergy Corporation	Agree with proposed method	Preference is to keep all electronic access requirements together, all physical access requirements together, and all informational access requirements together, but keep the three separate from each other.

#	Organization	Yes or No	Question 19 Comment
19.9	San Diego Gas and Electric Co.	Agree with proposed method	SDG&E recommends separation of the concepts of Logical (electronic) and Physical access.
19.10	APPA Task Force	Agree with proposed method	The APPA Task Force agrees with the SDT's proposal to separate requirements for Physical Access and Electronic Access. We do want to point out that both are interdependent. If a BES Facility has physical access control and does not have external routable connectivity, you do not need cyber system access control. This is covered in our comments for a number of the requirements where we recommend changing the impact level from "Required" to "Required for Routable External Connectivity Only."
19.11	Madison Gas and Electric Company	Agree with proposed method	The separation allows for clarity in these two distinct areas.
19.12	Progress Energy - Nuclear Generation	Agree with proposed method	To improve this Requirement, see attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
19.13	Xcel Energy	Agree with proposed method	We believe the separation is beneficial because it recognizes cases where physical access is needed but electronic access is not required, such as in the case for a mechanical maintenance vendor who performs no duties requiring electronic access.
19.14	Regulatory Compliance	Agree with proposed method	Would not want the controls for Physical Access and Electonic Access to be mixed.
19.15	US Bureau of Reclamation	Combine Access	Agree, but physical, logical, and information access control requirements should all be

#	Organization	Yes or No	Question 19 Comment
		Control requirements	included under a single set of requirements.
19.16	ERCOT ISO	Combine Access Control requirements	All access control areas should be combined (i.e., electronic access, physical access, information access). This will enable ease of use of the standard and a clearer understanding of the requirements. The current practice of having to go from standard to standard to find the requirements makes it more likely to miss a requirement and risk potential violations.
19.17	Puget Sound Energy	Combine Access Control requirements	As stated in the comments for question 18, Puget Sound Energy would prefer to see consistency (or an explanation of the differentiation of physical and logical controls).
19.18	Detroit Edison	Combine Access Control requirements	Combine all access control and revocation requirements into one requirement and one table.
19.19	Garland Power and Light	Combine Access Control requirements	Combine Tables R5, R9, R13, and R24.4 into one table so one can look at one table and see all the “revoke” requirements in one place - for most companies, the same people are going to be involved with “revoking” regardless of the Requirement #.
19.20	Consultant	Combine Access Control requirements	If the requirements for access control are the same, then combining them is better.Consideration should be given to combining information protection access and wireless access as well.It will also be clearer if there are any differences in access requirements for different types of access to have them combined so differences are obvious.
19.21	Idaho Power Company	Combine	It makes sense to combine some of them such as authorization, PRA and training,

#	Organization	Yes or No	Question 19 Comment
		Access Control requirements	revocation. Others are more specific to the type of access and may not lend themselves to combining.
19.22	USACE - Omaha Anchor	Combine Access Control requirements	Makes it easier to know which access must be terminated without looking through the entire document.
19.23	Southern California Edison Company	Combine Access Control requirements	The drafting team may not have adequately addressed the intent of Order 706 with respect to system security controls. Local logical (electronic) access is and should be recognized as a type of role based access where one has to be physically present near a device to operate it. The boundary protection for this type of role is (a) the physical security boundary and (b) the device level electronic security boundary. The proposed standard as it is currently worded allows for the removal of at least one access mechanism at the time of revocation. In that case, removal of access through the physical boundary will ensure the immediate revocation of a component critical for this type of role. The drafting team should add additional revocation criteria to adequately address this type of revocation.
19.24	Reliability & Compliance Group	Combine Access Control requirements	Tracking is easier if they are combined. We suggest that information access control be also included.
19.25	American Municipal Power	Combine Access Control requirements	Whenever possible, please eliminate redundancy in the requirements.
19.26	Progress Energy (non-	Combine	Will these be two distinct groups or will many have both accesses? Many people with

#	Organization	Yes or No	Question 19 Comment
	Nuclear)	Access Control requirements	physical access to transmission facilities will also need electronic access, suggesting that a single group/list may be easier to maintain.
19.27	Florida Municipal Power Agency	Combine Access Control requirements	Without a change in the definition of BES Cyber System to include an exclusion similar to the existing CIP-002-2 R3.1, R3.2 and R3.3, then there can be thousands of digital relays covered by this standard. A relay technical could have electronic access to thousands of such relays. It would be impossible to change all of those accounts within the time limits proposed in R9. We need to be careful in developing the standards that we do not cause unintended consequences of changing behavior that would reduce the reliability of the BES. This requirement R9 (and others within the standard) may have an unintended consequence of causing entities to revert to electro-mechanical relays to avoid onerous requirements in the standards. Reverting to electromechanical relays would likely increase costs as far as increased maintenance and testing requirements, but, would save costs of having to change accounts at numerous remote locations every time an employee changed positions.FMPA suggests combining physical and electronic (including wireless) access requirements to develop more reasonable requirements for situations such as these, e.g., revoking physical access to BES Cyber Systems with no external routable protocol should be enough. Thinking through these combinations is important to developing reasonable requirements.

20. Requirement R8 of draft CIP-011-1 states "Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 – Account Management Implementation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R8? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each criteria as represented in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R7 and R8 have been moved to CIP-004-5 and CIP-007-5.

Some commenters expressed confusion regarding the definition of "monitor" with respect to shared and guest account access privileges. In response, the specific term "monitor" has been removed from these account access requirements in favor of clearly defining the functions and actions associated with monitoring. Requirements to monitor access control have been moved to the Security Event Monitoring requirements in CIP-007-5.

Some commenters expressed a belief that the requirement for quarterly review of accounts and access privileges is excessive. The SDT notes that the quarterly review is required for Medium and High Impact BES Cyber Systems. The drafting team has clarified that it is not necessary to perform a detailed quarterly review of entitlements at the individual asset level.

Some commenters expressed a need to make the requirements for Account Management Specifications (CIP-011-1 R7) and for Account Management Implementation (CIP-011-1 R8) more consistent. In response, the drafting team has attempted to supply consistency as suggested by the commenters and has included these requirements in CIP-007-5.

Some commenters suggested removal of allowance of "guest" accounts. The drafting team believes there are reasons to retain "guest" accounts, and that complete removal would cause a hardship to some entities or may not be possible. Those using such accounts should be identified as required in the modified requirement.

Some commenters suggested combining Account Management Implementation (CIP-011-1 R8) with Access Revocation (CIP-011-1 R9). The drafting team has combined requirements in all cases where it seems feasible. However, what was formerly R9 concerned revocation, which carries a different VRF than most other access control requirements, and the subject matter concerns personnel actions. The Access Revocation requirements are now defined in CIP-004-5 R7.

Some commenters suggested changing R8.3 to "maintain a list of those who have access to guest/shared accounts." After review, the SDT determined that this part of the requirement was unnecessary and has removed it.

#	Organization	Yes or No	Question 20 Comment
20.1	National Rural Electric Cooperative Association (NRECA)		In R8.3, how do your demonstrate "monitor" to an auditor? This should be reworded such that both the auditor and the utility understand this the same way.
20.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
20.3	The Empire District Electric Company	Agree	Comments: Note impact level comments under question 21.
20.4	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.”Apply criteria” is not a strong requirement. The activity is account management, so, the requirement ought to be account management and R7 and R8 can be combined.Quarterly reviews of all accounts and privileges could be an onerous activity, and could actually decrease the reliability of the BES due to the higher rate of human error. FMPA suggests annual review of accounts and associated access privileges.
20.5	Puget Sound Energy	Agree	Puget Sound Energy suggests that R8.1 include wording regarding the removal of accounts. Example: “Establish and implement a process for authorizing the addition of account(s) and associated access. This process shall include necessary steps for the removal of accounts when no longer necessary.”
20.6	Progress Energy - Nuclear Generation	Agree	R8 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
20.7	APPA Task Force	Agree	The APPA Task Force Agrees with the criteria. See our response to Question #21 for

#	Organization	Yes or No	Question 20 Comment
			the Impact Levels discussion.
20.8	FEUS	Agree	The drafting team should clarify 8.3 what is intended to 'monitor' the use of shared and guest accounts.
20.9	Bonneville Power Administration	Agree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Item 8.2 in Table R8 states "Conduct a quarterly review and verification of accounts and associated access privileges." It does not indicate what type of documentation is required to demonstrate compliance. Is an attestation sufficient documentation? Or is the Responsible Entity required to have specific documentation of its quarterly review by account types, etc?
20.10	Reliability & Compliance Group	Agree	The requirements in table 8 really should apply to medium impact systems as well.
20.11	Independent Electricity System Operator	Disagree	- R8.3 is anonymous synonymous with null sessions? If so then this will be difficult since anyone in the same network can connect with a null session.
20.12	Southwest Power Pool Regional Entity	Disagree	8.1: Authorization should be required for both the addition and the modification of a user account. 8.3: Define what is meant by "monitoring" the use of the shared and guest/anonymous accounts. Is it sufficient to know that someone used the account or must their activities with the account be monitored? Is monitoring required in real-time or after the fact? Is there a requirement to review account activity after the fact?
20.13	Con Edison of New York	Disagree	8.2 Quarterly reviews are excessive, suggest annual reviews and a documented

#	Organization	Yes or No	Question 20 Comment
			process for adding, removing or modifying access8.3 Need clarification on what monitoring means outside of annual review of if it is still required
20.14	Progress Energy (non-Nuclear)	Disagree	8.2 Quarterly seems to be too frequent - propose 6 months or longer. We are required in R9 to revoke access for those that are terminated or do not need access within 72 hours.
20.15	American Electric Power	Disagree	8.3, regarding "Monitor the use of shared and guest/anonymous accounts". This is not technically feasible on all systems. What level of detail is required to monitor the use? Does this need to be an automated electronic process? Is it even feasible to believe this can be done manually? How long must this monitoring data be kept?This should be removed.
20.16	Michigan Public Power Agency	Disagree	A quarterly review and verification of accounts would be overly burdensome and would not improve the electronic security of the system compared to a defined "annual" review.
20.17	BCTC	Disagree	Â Suggest removing “guest” from the language; guest accounts should not be permitted to be used in a secure systemÂ R 8.3 why single out monitoring of shared and guest accounts; should we not monitor all accounts?; unsure what the objective of this requirement is
20.18	Entergy	Disagree	Again, this is similar to NEI-08-09 Rev 6 Section 1.2. However, we question the advantage of having Account Management Implementation separate from Access Revocation. Please consider combining R9 with R8 by adding requirements 8.4 and 8.5 (below) and modifying the language in 8.1, as well as adding ‘required’ to low and medium impact BES Cyber Systems for 8.2 and 8.3.
20.19	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes a technical feasibility exception may be required base on the current wording of this requirement when considering local access to programmable electronic devices in a substation environment that do not

#	Organization	Yes or No	Question 20 Comment
			support the ability to demonstrate acceptable use.
20.20	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing the wording of R8.3 to read:"Maintain a list of who has access to shared and guest/anonymous accounts."
20.21	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, an account management process should be required at the same levels.
20.22	LCEC	Disagree	In 8.1, changes to existing accounts that grant additional access should be authorized as well.
20.23	Black Hills Corporation	Disagree	In 8.2, quarterly is a good goal, but without a solid definition of the window associated with "quarterly", this will be an evidence gathering problem - suggest changing to semi-annual.
20.24	Minnesota Power	Disagree	In Part 8.3 of Table 8 the Standards Drafting Team needs to clarify what is meant by the term "monitor." Does this mean that Registered Entities need to be able to review who (named individual) accessed a shared account, and when this access occurred, or does this require logging their actions while utilizing the shared account? In addition, does this include system/admin accounts (as they are listed above as being different than shared accounts)? These measures seem to be appropriate, but implementation and providing auditable evidence could be difficult.
20.25	Idaho Power Company	Disagree	Monitor in 8.3 is vague. Would it require just that we know who used the account when or more detail about what the user did while using the account.
20.26	National Grid	Disagree	National Grid recommends changing Requirement 8.2 from "quarterly review" to "annual review" since the extra work is noticeably less than the benefit. Request clarification on 8.3 "monitor"
20.27	NextEra Energy	Disagree	NextEra believes the standard requirement 8.3 needs to be clarified regarding the

#	Organization	Yes or No	Question 20 Comment
	Corporate Compliance		ability to "Monitor" the use of shared and guest/anonymous accounts. What is the extent of this monitoring? If allowed by the standard, we do not believe effective monitoring of the use of these generic accounts is feasible due to their generic nature. This may be better stated as maintaining logging information and ensuring that quarterly reviews ensure access is documented to individuals with valid business need and credentials.The impact levels are appropriate for the requirement. However, for Requirement 8.2 it is unclear what an acceptable verification method is. Clarification regarding recommended methods for verifying accounts and privileges especially for legacy BES Cyber System components should be included in the requirement.Additionally, Requirement 8.3 is concerning because it is unclear what monitor means in the context of the requirement, the word should be clearly defined. Multiple users can use shared accounts at the same time and that would be something impossible to monitor. If monitor means who has approval to use shared accounts and who is has access to the password for shared accounts that should be defined in the requirement. Likewise, it is unclear how to monitor anonymous access. Clarification should be provided regarding the definition, intent, and appropriate evidence to demonstrate monitoring.
20.28	Oncor Electric Delivery LLC	Disagree	Not all BES Elements can monitor the use of shared and guest/anonymous accounts. TFE should be applicable. Requirement 8.3 should only apply to remote routable communications.
20.29	American Municipal Power	Disagree	Please provide a little or no impact level category
20.30	Pepco Holdings, Inc. - Affiliates	Disagree	Please reference to question 17.
20.31	Ameren	Disagree	R8.2 - Exhaustive review of all accounts quarterly will be time consuming with no added protection to the BES; this requirement should be changed to annually.

#	Organization	Yes or No	Question 20 Comment
20.32	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R8.2. Due to the requirements of R9 the review and verification time should be extended to an annual time frame.
20.33	Western Area Power Administration	Disagree	R8.3 - What constitutes “monitoring” of the use of shared and guest/anonymous accounts?
20.34	EEI	Disagree	R8.3 may create the possibility that an Entity would have to be able to show who used a shared account or password each time that it was used. This is an unimplementable requirement; the requirement should be clarified to make it clear that what must be tracked is the ability to use the shared account.
20.35	Southern Company	Disagree	R8.3 may create the possibility that an Entity would have to be able to show who used a shared account or password each time that it was used. This is an unimplementable requirement; the requirement should be clarified to make it clear that what must be tracked is the ability to use the shared account. In addition, . this requirement could require a large number of TFE’s for systems which do not support multiple passwords.
20.36	Kansas City Power & Light	Disagree	R8.3: What does the “Monitor” represent?
20.37	Hydro One	Disagree	Recommend changing Requirement 8.2 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Request clarification of the use of “monitor” in 8.3.
20.38	ISO New England Inc	Disagree	Recommend changing Requirement 8.2 from “quarterly review” to “annual review” since the extra work is noticeably less than the benefitR8.3 is anonymous synonymous with null sessions? If so then this will be difficult since anyone in the same network can connect with a null session. clarification on monitoring use of shared accounts.

#	Organization	Yes or No	Question 20 Comment
			"use" not provisioning. login/logout, all activity while logged in? commands used?
20.39	Northeast Power Coordinating Council	Disagree	Recommend changing Requirement 8.2 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Request clarification of the use of “monitor” in 8.3.
20.40	BGE	Disagree	Replace the word “elements” with Cyber System Component to maintain consistency with the defined terms. R7 & R8 requirements need to be synchronized. What is the definition of “monitor” (track actions, how much detail, will sudo suffice?)
20.41	Northeast Utilities	Disagree	Request clarification:- Are shared accounts included in 8.2 and required to be reviewed quarterly?- What does monitor mean in 8.3?
20.42	Garland Power and Light	Disagree	Requirement 8.3 - Do not believe that shared and guest/anonymous accounts should be allowed.
20.43	Network & Security Technologies Inc	Disagree	SDT should clarify intent of 8.3 (monitor use of shared and guest/anonymous accounts).
20.44	GE Energy	Disagree	Some type of account and privilege review should be required for Medium Impact systems, but not on a quarterly basis. These systems may well be used to validate software before promoting it to High Impact systems, and thus should have some account management due diligence.
20.45	Platte River Power Authority	Disagree	Suggested Revision:8.3 Track individuals that have been granted access to shared and guest/anonymous accounts.
20.46	Duke Energy	Disagree	Table 8: 8.2 quarterly reviews are too frequent. Suggest annually8.3 explain what is meant by “Monitor”What are the expectations for monitoring use of shared and guest/anonymous accounts? Is that up to the Responsible Entity? If the RE provides a procedure/policy and follows the policy, is that sufficient to pass audit?What is the

#	Organization	Yes or No	Question 20 Comment
			acceptable practice? 24/7?
20.47	ReliabilityFirst Staff	Disagree	Table R8; row 8.1 - suggest adding the word “document”, row 8.2 - what constitutes “review” and suggest the review should be documented, row 8.3 - what does “monitor” mean?
20.48	Constellation Energy Control and Dispatch, LLC	Disagree	The phrase "monitoring the use" of accounts is too vague.
20.49	ERCOT ISO	Disagree	The requirements of R7 and R8 can be combined. The purpose of each requirement is so similar that there appears to be no reason to separate them.
20.50	WECC	Disagree	The table lists three procedures for account management. Suggest this requirement be written to state: “Each Responsible Entity shall have implemented and documented procedures as described in Table...”The requirements should mandate additional rigor around access management, including the maintenance of access lists or automated provisioning systems. Additional specificity should be added to clarify the level of detail at which access must be tracked.
20.51	Consultant	Disagree	The word 'criteria' should be changed to requirements, as the table is listing requirements.Suggest replacing the words "to prevent malicious operation of BES Elements by maintaining..." with to maintain control..."Table R8-8.3 Not clear why this only applies to shared and guest accounts? And the difference between 'monitoring' and 'logging' is not clear.Suggest requirement is to "Log electronic access to BES Cyber Systems." and keep as required for High Impact Systems.
20.52	Dairyland Power Cooperative	Disagree	Validating whether users are assigned to appropriate roles or accounts should follow this timing. A detailed review to insure that the roles (or account groups) have proper permission settings can be a very time consuming and complex task depending on the complexity of a system. The detailed role definition review should be no more frequent than annually. The language used is not clear as to whether a distinction is

#	Organization	Yes or No	Question 20 Comment
			intended.
20.53	GTC & GSOC	Disagree	We recommend in R8.3 the term "Monitor" be replaced by "Review monthly". The term "monitor" could be taken to imply real time monitoring. Many entitities do not have the communication links required to meet such a real time requirement.
20.54	Alliant Energy	Disagree	We recommend retaining the annual requirement for 8.2 account review while retaining a quarterly requirement for personnel access review.8.3 needs more clarification regarding the activities included in the term “use” so as to provide specific guidance as to what constitutes a sufficient audit record.
20.55	The United Illuminating Co	Disagree	What is the intent of 8.3? It is difficult to discern what Monitor means in this requirement.
20.56	Manitoba Hydro	Disagree	word “Monitor” in Requirement 8.3 is unclear.

21. Table R8 provides direction concerning what impact level of BES Cyber Systems to which Requirement R8 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R8 has been moved to CIP-007-5 R5.

Some commenters expressed concern CIP-011-1 R8.1 (Account Authorization) should apply to all three impact levels. In response, the SDT notes that authorization also implicitly carries with it requirements for account review, revocation, and training. The SDT did not believe that the effort required to comply with these requirements for all three impact was appropriate given the risk posed to the Bulk Electric System.

Other commenters expressed concern that only Medium Impact BES Cyber Systems with routable external connectivity should be subject to the Table R8 requirements. The SDT disagrees and believes regardless of a BES Cyber System's communication characteristics, it is important to ensure that access to BES Cyber System is properly authorized and subject to periodic review.

Other commenters also expressed concern that the requirements in Table R8 should be aligned with those in Table R7. In response, the Table 7 and Table 8 requirements have been combined into CIP-007.

Some commenters expressed that the impact levels in R8.2 should have different review periods. The SDT believes a quarterly review period for access authorization and an annual review period for access privileges are appropriate for both High and Medium Impact BES Cyber Systems.

#	Organization	Yes or No	Question 21 Comment
21.1	Florida Municipal Power Agency	Agree	For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections.
21.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.

#	Organization	Yes or No	Question 21 Comment
21.3	Puget Sound Energy	Agree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management. If account management is not required for Low Impact BES Cyber Systems then it is unclear what benefit is there in identification of those accounts.
21.4	Progress Energy - Nuclear Generation	Agree	R8 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
21.5	Progress Energy (non-Nuclear)	Agree	See comment 14.
21.6	FirstEnergy Corporation	Agree	While the proposal provides flexibility based on Impact Categorization from a practicality viewpoint it will be easier to administer if all are treated equally. FE would likely take a conservative approach and treat all the same to simplify administration of this requirement.
21.7	ReliabilityFirst Staff	Disagree	8.1 should apply to all BES Cyber Systems. 8.2 should provide different periods of review for different levels of impact. Suggest making these annual for Low Impact, semi-annual for Medium Impact, and quarterly for High Impact.Suggest “required” Medium Impact for row 8.3.
21.8	ERCOT ISO	Disagree	8.1: Should be required for all. 8.2: Could be documented temporally. Low Impact required annually. Medium Impact required quarterly. High Impact required quarterly. 8.3: Please clarify meaning of “monitor”. Should be revised to address who has access to the accounts.
21.9	US Army Corps of Engineers, Omaha Distirc	Disagree	8.3 "monitor the use of" is somewhat vague. What would the measure be? Please define

#	Organization	Yes or No	Question 21 Comment
21.10	Southwest Power Pool Regional Entity	Disagree	Account authorization is a basic security control and should be applicable at all impact levels. Periodic review is also important and should be done for at least Medium impact systems as well, albeit more frequently for High impact than lesser impact.
21.11	Alliant Energy	Disagree	Alliant Energy agrees with EEI's comments relative to 8.3 and the consideration of capabilities and connectivity.
21.12	USACE HQ	Disagree	At a minimum, 8.2 should be required for all impact levels. Requirement 7 creates a document of every account type and its acceptable use, but for low and medium impact systems it is not required to update the same as per requirement 8.2.
21.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
21.14	The Empire District Electric Company	Disagree	Comments: For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
21.15	FEUS	Disagree	Disagree: The drafting team should consider 8.1 be applicable to LOW BES Cyber Systems for consistency with 7.1, 7.2, and 9.1. Without a process for authorizing new accounts it is difficult to review approved accounts and to revoke access that was not authorized.
21.16	WECC	Disagree	Even "Low Impact" systems have the capability of impacting operation of the BES within 15 minutes, thus these requirements should be required for all impact levels. Again, this requirement could then be rewritten without the table to provide more clarity.These requirements should apply to all impact levels

#	Organization	Yes or No	Question 21 Comment
21.17	San Diego Gas and Electric Co.	Disagree	For entities that own both Medium & High impact assets, they will likely perform all of the requirements contained in Table 8 for both classes of assets instead of maintaining separate procedures and mechanisms that will have a higher risk of compliance errors. SDG&E believes it just adds potential confusion to the process to have different requirements for Medium and High impact assets in this instance.
21.18	MRO's NERC Standards Review Subcommittee	Disagree	For item 8.1 through 8.3, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
21.19	American Transmission Company	Disagree	For R8.1 through R8.3 suggest adding "Required for routable external connectivity only." At the present there is no practical method to monitor the use of devices such as relays and IMUXs when accessed from inside a substation. They may be able to be front-ended, but as yet it has not proven viable.
21.20	Consultant	Disagree	If 8.1 requires authorizing accounts for Medium Impact Systems, then quarterly review of 8.2, and the logging access of 8.3 (see previous comment) should be required for those systems.Or, remove the requirement in 8.1 for Medium Impact Systems.
21.21	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, an account management process should be required at the same levels.
21.22	Black Hills Corporation	Disagree	In 8.3, do not understand why guest/anonymous accounts would be allowed. Should be limited to shared accounts only.
21.23	E.ON U.S.	Disagree	It is not clear what is meant by the term "monitor." Does monitor in 5.2 mean active

#	Organization	Yes or No	Question 21 Comment
			monitoring, e.g., video" Does it mean log?
21.24	Emerson Process Management	Disagree	It is prudent that account and privilage can only be created and granted with proper authorization. This principal should be applied to any BES Cyber System.
21.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
21.26	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's comments below:Regarding Table R8 Row 8.1:There can be a documented process even for low impact systems. It may not be as rigorous as for medium or high impact systems.Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.27	Con Edison of New York	Disagree	Modified 8.2 should be required for medium (annual review)
21.28	American Municipal Power	Disagree	Please provide a little or no impact category
21.29	BGE	Disagree	R7 & R8 requirements are not synchronized.
21.30	Ameren	Disagree	R8.3 - should be required for Medium Impact Systems.
21.31	Allegheny Energy Supply	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.

#	Organization	Yes or No	Question 21 Comment
21.32	Allegheny Power	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.33	EEI	Disagree	Regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.
21.34	Southern California Edison Company	Disagree	SCE believes it may be possible to leverage the NERC PRC standards to effect compliance. In R8.2, an additional control with a timeframe longer than a quarter may be added for low and medium impact systems. It seems that access to low and medium impact systems never has to be verified. Although monitoring under R8.3 is not required for low and medium, which SCE is in agreement with, SCE believes that R8.2 should be modified where list of accounts and access privileges are tracked on a time bound basis.[MVL-HOW?] This may be an opportunity for the drafting team to review the appropriate NERC PRC standard on protection relay maintenance schedules and leverage the compliance requirements stated there.
21.35	GE Energy	Disagree	See question 20 comments
21.36	Entergy	Disagree	Suggest 8.2 apply to medium assets as 8.1 required a process for authorization. There is value in reviewing access lists from a security perspective.
21.37	Network & Security Technologies Inc	Disagree	Suggest adding a periodic review of access privileges to Medium Impact systems (8.2), perhaps every 12 months in lieu of quarterly.

#	Organization	Yes or No	Question 21 Comment
21.38	Alberta Electric System Operator	Disagree	The AESO believes that reviews should also be performed for Low and Medium Impact levels. Consider creating additional rows in the table to perform annual reviews for Low and Medium Impact BES Cyber Systems.For Table 8.1 - A process should be required for all impact levels.For Table 8.3 - Monitoring should be performed for all impact levels, however frequency of monitoring can be dependent on the impact level.
21.39	APPA Task Force	Disagree	The APPA Task Force supports the proposal by the MRO-NSRS to change 8.1 - 8.3 under Medium Impact to read "Required for routable external connectivity only." As stated in our response to Question #19, the physical security is covered in requirement R5 so only routable external connected devices are vulnerable. The tables should therefore read:R8 Table 8.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR8 Table 8.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: RequiredR8 Table 8.3: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required
21.40	Constellation Power Source Generation	Disagree	The impact levels mapped out in R8 should be changed to mimic those in R7. Why identify all account types for every BES Cyber System, but then require processes for authorization and quarterly reviews of privileges for some of the impacts?
21.41	Reliability & Compliance Group	Disagree	The requirements in table 8 really should apply to medium impact systems as well.
21.42	Southern Company	Disagree	The scoping levels of R7-R14 are vastly expanded when compared to R5 and R6. Each requirement should be examined to determine the correct scope to best support overall reliability. The lack of differentiation based on connectivity and BES component type, in conjunction with the inclusion of requirements that have a per-low-system-component impact, mean that the vast majority of the effort involved in CIP compliance will have to be spent on low-impact, relatively unimportant assets,

#	Organization	Yes or No	Question 21 Comment
			often at the expense of overall reliability.
21.43	Oncor Electric Delivery LLC	Disagree	These requirements should only apply to systems with routable communications.
21.44	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding Table R8 Row 8.3.
21.45	We Energies	Disagree	We Energies agrees with EEI regarding Table R8 Row 8.1:There can be a documented process even for low impact systems. It may not be as rigorous as for medium or high impact systems.We Energies agrees with EEI regarding Table R8 Row 8.3:There needs to be consideration of capabilities and connectivity options for different devices. For example, devices without external connectivity or that use non-routable protocols may not be able to provide monitoring functionality. Moreover, even devices that use routable protocols may not have the ability to provide information about account use.

22. FERC has mandated immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset. Requirement R9 of draft CIP-011-1 states "Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 – Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R9? Please explain and provide any suggestions for modification, including time proposals. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R9 has been moved to CIP-004-5 R6 and R7.

A number of commenters requested that the Standards make a distinction between "primary" access and "secondary" access, based on an understanding that an individual would need primary access to be able to use any secondary access (such as a database account). The SDT has revised the access revocation requirements (CIP-004 R7) to state that revocation of access includes remote, electronic, and physical access to the BES Cyber Systems. The requirements also address the revocation of "the ability to access" BES Cyber Systems and BES Cyber System Information as well as the resulting follow up actions related to additional assets (such as applications and databases). The SDT believes this best captures the concept of primary and secondary access.

Other commenters suggested revocation "with cause" should remain at 24 hours, and revocation "without cause" should remain at 7 days. This timing would keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer. In response, the SDT notes the FERC Order directs revocation of access to occur immediately in all cases where access is no longer needed. The requirement has been modified to simply revoke access when a person no longer needs it. Given that organizations usually have termination procedures to return company property and perform exit interviews, the SDT believes the processes for revoking access (both physical and remote electronic) can be incorporated into an organization's termination and transfer procedures.

Some commenters expressed concern that the revocation timeframe requirements based on combinations of BES Cyber System type and Impact Level are overly complex, and add confusion and undue administrative overhead in situations of job changes. To address this, commenters recommended more consistent timeframes. In response, the requirement has been modified to simply revoke access when a person no longer needs it. Evidence showing termination down to the hour is not practical in many cases. In the revised requirements, entities will show revocation of access as part of their termination procedures and demonstrate they follow these procedures (i.e., through dated sign-off records, system logs or actual system access control databases).

#	Organization	Yes or No	Question 22 Comment
22.1	Green Country Energy	Agree	Additionally addressing the transfer of responsibilities to another individual shpould be addressed if the terminated employee is a system administrator or such. If a "key" individual is terminated it may be quite a process to remove them from the system within 24 hours,leaving a system vulnerable or a backup plan unable to be executed. In summary termination with cause of a high security level employee could be very difficult to accomplish in 24 hours.
22.2	Oncor Electric Delivery LLC	Agree	One of the few examples where “Control Center” is separated from Transmission and Generation.
22.3	FEUS	Agree	The drafting team should consider revising the wording for revocation as ‘immediately but not to exceed XX hours’
22.4	Progress Energy - Nuclear Generation	Agree	To improve implementation of this requirement incorporate information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
22.5	Regulatory Compliance	Disagree	9.1 - clarify for service vendor that the clock should start upon notification to the entity.9.2-9.4 - 7 day revocation across the board
22.6	American Electric Power	Disagree	9.2 - 9.4: Recommend rewording 9.2-9.4 to match 5.7-5.9 or vice versa.Recommend removing physical access and external connectivity within a short-time window, and application rights later.
22.7	ISO New England Inc	Disagree	9.2, 9.3, 9.4 - all should be within the same time frame 72 hours. Same level of security issues or concerns across all (control center, trans, gen). Remove Requirements 9.3 and 9.4R9.2, R9.3 a d R9.4 suggest changing the requirement to “Review access to BES Cyber Systems for personnel that change job responsibilities as a result of reassignment, transferred to other positions within x hours of the

#	Organization	Yes or No	Question 22 Comment
			change."The purpose of the requirement is so that personnel have the least amount of access that is needed to do their jobs and so that they don't accumulate access as they move around. Also this is to limit possible segregation of duty violations and to require that authorized access permissions are the minimum necessary to perform work functions. (R10.6)
22.8	Dominion Resources Services, Inc.	Disagree	9.2, 9.3, and 9.4. To meet regulatory directives, if job duties are changed due to disciplinary actions or are "forced" on the user then a shorter time frame may be necessary. However, the current 24 hour time period is the least time period that can be reasonably accommodated through the business processes. And 24 hours is only possible if Revoking System Access is limited to controls that prevent the user from physically and electronically accessing the system. For example, if the user must either have physical access to the device or authenticate through a corporate system (e.g., active directory) before being allowed to access a BES Cyber System, then removal of physical access rights and of the ability to authenticate in the corporate system meets the Requirement for revoking system access, even though an account may still exist on the BES Cyber System. The account on the BES Cyber System would be removed within 7 days since many BES Cyber Systems are not administered 24x7.Requirement R4 establishes the process for personnel risk assessments. This practice determines the loyalty, reliability and trustworthiness of an individual as a prerequisite to authorizing logical or physical access. This is a standard practice used throughout the physical and cyber security industry and accepted by other regulatory agencies and Federal programs. Similar to R4.3, personnel risk assessments typically must also re-validate this trustworthiness periodically - commonly within 7 years and in some cases more frequently depending on the nature of the access. The presumption is that, once trustworthiness is established, it is not invalidated unless there is cause to reconsider or an individual voluntarily terminates their employment or retires. Only in instances where the established trustworthiness is in question, is prompt access revocation appropriate and warranted. Consequently, for personnel who "no longer require access", but for which there is no cause to question their trustworthiness, there is no basis for immediate or prompt revocation of access

#	Organization	Yes or No	Question 22 Comment
			within the time frames specified in this standard. The DHS Catalog for Control System Security Controls, Sections 2.3.4 and 2.3.5 reflect this practice - requiring revocation of access for cause within 24 hours and revocation of access for personnel reassigned or transferred to another position within 7 days. In other regulatory programs, revocation of access, not involving a question of change in trustworthiness, is handled via a periodic (e.g., monthly) review of access only. The 7 day requirement in the current standards would meet or exceed standard practice in this case. The requirements should be clarified to state that if there is no triggering event indicating that access is no longer required, then that determination can be made at the quarterly review.
22.9	Con Edison of New York	Disagree	9.2,3,4 - may be dependent on a company's existing HR/Payroll business system capabilities and introduce significant costs to remediate. Even though the individuals were trusted and the trust did not change as a result of cause. A week may be more realistic
22.10	US Bureau of Reclamation	Disagree	A requirement for revocation needs to be included for all impact levels. Suggest the timeframes for Requirements 9.2 through 9.4 be established on the basis of business days (for example 2 business days) or that the number of hours be increased cover long weekends.
22.11	MidAmerican Energy Company	Disagree	Access removal should be considered complete by removing physical and remote access. Removing physical and remote access effectively removes access to any BES Cyber Systems. Also see MidAmerican Energy's response to question 54.
22.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.Also, 9.2 - 9.4 is the second of many occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations

#	Organization	Yes or No	Question 22 Comment
			for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
22.13	Kansas City Power & Light	Disagree	Are these requirements applicable for electronic and physical access? 36 and 72 hours are too short a time frame for considering personnel who have changed access status other than that of termination when consideration of weekends and holidays. 5 to 7 business days would be an appropriate time frame. For personnel terminated for cause, 24 hours is acceptable.
22.14	Xcel Energy	Disagree	As noted in our response to a previous question, the 36 and 72 hour timeframes to revoke unescorted physical access for individuals no longer requiring access under 5.8 and 5.9 are not justified. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not warranted.
22.15	E.ON U.S.	Disagree	CIP-011-1, R9 references "system access." Does this mean physical or electronic access? For requirements 9.3 an d 9.4 it can be difficult to determine the exact time a person no longer needs access if, for example, the person has not required access for an extended period of time.E.ON U.S. does not believe compliance requirements are necessary for the low impact category.
22.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
22.17	The Empire District Electric Company	Disagree	Comments: If physical access is removed per R5, and remote access is removed per R13, this effectively removes all avenues to electronic access. Therefore, we propose

#	Organization	Yes or No	Question 22 Comment
			that the period for removing electronic access be lengthened.
22.18	BGE	Disagree	Define “immediate”. The table does not specify that the revocation is for personnel with electronic access. Combine 9.2, 9.3 & 9.4 revocation for any high impacted system should be consistent.
22.19	USACE HQ	Disagree	Does not make sense to create “for cause” requirement in any environment but a “no longer require” for only three (3) specific environment. I suggest to only have a two requirements, one (1) “for cause” and one (1) “no longer require”.
22.20	Duke Energy	Disagree	For 9.2, change 36 hours to 48 hours. Is the FERC mandate for ALL BES systems? Is there any room for loosening the requirement for low impact system?
22.21	Reliability & Compliance Group	Disagree	For personnel transferring to new positions where access is no longer available, 36 hours seems unduly burdensome. Recommend that this be changed to 72 hours for personnel no longer needing access to control center BES Cyber Systems.Also, this contradicts R5. Why do you need to revoke physical access at all for medium impact systems if you did not authorize it in the first place?
22.22	LCEC	Disagree	I agree with the intent of this requirement but need additional clarification to determine what is meant by revoking system access. Access may be granted at a system or component level. If system, network & wireless access is removed is this requirement satisfied? If audited at the component level, it may not be possible to make all of the necessary changes within the timeframes that are being dictated. The scope of this requirement should be clarified to indicate remote or wireless access only. Component level access will be mitigated by the physical security controls.
22.23	MRO's NERC Standards Review Subcommittee	Disagree	If physical access is removed per R5, and remote access is removed per R13, this effectively removes all avenues to electronic access. Therefore, we propose that the period for removing electronic access be lengthened.

#	Organization	Yes or No	Question 22 Comment
22.24	WECC	Disagree	If the goal is to revoke access at termination (“immediate”) then the requirement should state simply, “The Responsible Entity will remove electronic and physical access at the time of termination.” This should be possible for any entity that has use physical tokens for physical or electronic access (such as RSA SecurID, keys, RFID badges), however it would NOT be possible for entities that are still using access control systems with passwords, combination locks, or other access methods where revoking access requires reprogramming of devices. Note- this could indirectly require token based authentications for perimeter access which is not necessarily a bad requirement for medium and high impact systems.Terminations for cause should require immediate revocation of access - performed in conjunction with the termination notification to the employee. This is already standard practice at many entities. Additional criteria regarding employee suspensions should be added.
22.25	Consultant	Disagree	Immediate revocation is not achievable as indicated by the fact that there is a time frame for each identified revocation condition. Suggest using rules similar to the nuclear plants for access revocation, as those rules have over 30 years of regulatory basis for being adequate to control access revocation.R9. - Suggest deleting the words "...by maintaining control of access to its BES Cyber Systems," Revoking access does prevent malicious operation.9.1 - If access to Low Impact Systems does not require an authorization process(R8), then it is illogical to require the undocumented access to be revoked.9.1, 9.2, 9.3, & 9.4 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.9.2, 9.3, & 9.4 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.9.2, 9.3, & 9.4 - the word "such" in the statement is unnecessary. Suggest deleting the word "such".Similar to combining access requirements, the revocation requirements should be combined. This makes both

#	Organization	Yes or No	Question 22 Comment
			similarities and differences easier to understand.
22.26	Minnesota Power	Disagree	In extreme circumstances, it may not be possible to adhere to proposed the 24 and 36 hour revocation timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week or where notification of termination comes from corporate systems that are also updated on an 8 hours a day, 5 days a week schedule.Are we to interpret “revoke system access” to mean access to individual accounts, or does it also include shared/group/system/admin accounts known by the person who no longer requires access?
22.27	LADWP	Disagree	It is infeasible to revoke access to Medium and High BES systems within the max 72-hour requirement. a. Revocation of Hard-Copy information should not be considered under the standard. b. The current 7 day window for revocation of access for individuals no longer needing access is reasonable and should remain a part of the standard.
22.28	Allegheny Energy Supply	Disagree	It may be appropriate to address revocation of access within the context of “Effective Access.” For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Another example is if the BES Cyber System has no electronic communications outside of its physical boundary, then revoking physical access is effectively revoking access. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.29	Allegheny Power	Disagree	It may be appropriate to address revocation of access within the context of “Effective Access.” For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System.

#	Organization	Yes or No	Question 22 Comment
			Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.30	EEI	Disagree	It may be appropriate to address revocation of access within the context of "Effective Access." For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.31	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
22.32	Southwest Power Pool Regional Entity	Disagree	Make a distinction between "primary" access and "secondary" access. Primary access includes the domain user account, remote access (e.g., VPN, dial-up) credentials, and physical access (badge, keys) credentials. The idea is that the individual would need to gain access using the primary access in order to be able to use any secondary access such as a database account. Revoke primary access in much less than 24 hours for termination for cause, especially for control center systems access. Ideally, primary access should be revoked at the same time the individual is being terminated. Express revocation timeframes for terminations other than for cause in terms of business days. Provide for a negotiated "effective transfer date" other than the HR effective date; transferred personnel often back fill or otherwise continue to provide assistance to the losing department for some period of time.
22.33	National Grid	Disagree	National Grid recommends that Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems (transmission, generation, and control centers)

#	Organization	Yes or No	Question 22 Comment
			and remove Requirements 9.3 and 9.4.
22.34	Manitoba Hydro	Disagree	NERC should request from FERC a clarification on their meaning of “immediate”. “Remote access” in Requirements R11 - R14 could be considered a subset of “system access” in Requirement R9. Is the intent for Requirement R9 to refer to local, electronic access?
22.35	NextEra Energy Corporate Compliance	Disagree	NextEra believes the requirements for access revocation for personnel who are still employed by the responsible entity but no longer in a job function that requires access to BES Cyber Systems are too restrictive. The responsible entity should be able to develop timelines and processes to support the removal of access for a person who transfers, since a transfer is not an indication that the employee is a security risk or threat to the BES Cyber System.For personnel terminated for cause, the access should be removed before notification to the impacted personnel. The access that is revoked would be considered global access, as in the terminated personnel’s physical access to the BES Cyber Systems as well as network access. The responsible entities could then create a process, which gives them additional time up to two weeks, to remove individual system access to each BES Cyber system component. For personnel who separate from a responsible entity due to retirement or resignation should go thru a deprovisioning process based on the responsible entities internal processes. The risk posed by normal termination or transfer is extremely small and if malicious behavior or intent is planned, then the actions will happen before the scheduled termination. The recommendation is to revoke network and corporate cyber access and physical access, which would be considered global access within a 2-week timeframe. The responsible entities could then create a process, which gives them additional time up to thirty days, to remove individual system access to each BES Cyber system component. NextEra would also like to establish what is meant by revoking System Access? Is this revocation time frame applicable to removal of access rights at the Boundary Level, BES Cyber System level, or BES Cyber System Component Level?â€,Access is given to individuals on different levels beginning with access to entity networks and facilities, and flowing to access to individual BES Cyber System

#	Organization	Yes or No	Question 22 Comment
			components. The revocation of the individual's access to entity networks and facilities should be referenced or defined as accomplishing the desired result. This effectively removes the individual's ability to access any BES Cyber Systems and allows for the timely execution to approach the "immediate" completion as defined in Table R9.â€,This item should also reference upstream requirements to grant access at either the BES Cyber System level or the BES Cyber System Component level. What level of documentation is required for access rights?â€,Transmission Faciltities' IEDs (such as protective relays) utilitze shared passwords as the method of access control. What are the expectations regarding R9 - Access Revocations for those BES Cyber System Components? Are the expectations to change every IED shared password the user being revoked had access to in every High and Medium BES Transmission Facilities within 72hrs? This task of changing hundreds of protective relay passwords within 72hrs is currently not operationally feasible.R9 - indicates that NERC CIP password schemes will be applied to all units. Many systems with passwords have never had a password change.Large volume to manage. Control systems were not designed to have password changed regularly.When we implemented the NERC rules on the Load Control Computers in December, we found that they wouldn't run properly without the administrator password from when the software was originally installed. On one machine, we ended up having to reload the software to get it to work againThe OPC connections between the Toshiba ST and Ovation systems are the same way, they will only work with the logon credentials from the original software loading and configuration.NextEra suggests not requiring changes for legacy systems with embedded passwords.
22.36	PacifiCorp	Disagree	Per question 15 above, PacifiCorp believes revocation when access is no longer needed should be consistent among the different types of facilities. Specifically, R9.2 should be merged with both R9.3 and R9.4 resulting in a consistent 72-hour requirement.Access removal should be considered complete by removing physical and remote access. Removing physical and remote access effectively removes access to any BES Cyber Systems.

#	Organization	Yes or No	Question 22 Comment
22.37	American Transmission Company	Disagree	Propose maintaining time frame in 24 hour increments. Revocation for Medium impact should be revised from 36 hours to 48 hours.
22.38	Southern Company	Disagree	R9 should be modified to make it clear that the goal is effective removal of access - for example, that can be accomplished through revocation of physical access and revocation of network access without action at the individual BES Cyber System Component level.Removal of access within 24 hours for low-impact systems is unnecessarily burdensome.An unachievably short time limit for revocation due to dismissal for cause will actually result in damaging security as Entities are forced to delay dismissal until revocation can be accomplished in order to maintain compliance.Requiring that an Entity monitor the employment status of its contracting companies' employees creates an impossible burden. The requirement should be modified to require removal of access within a given number of hours after notification by the contracting company, combined with requirements that communication requirements are to be given to the contracting company.
22.39	Luminant	Disagree	R9 should not be required for low impact. 9.2 could 36 hours be changed to 48 (2 days) 9.3 and 9.4 1 week
22.40	Detroit Edison	Disagree	R9 uses the term "system access" while in other places the term is "authorized electronic access". Table entries 9.2, 9.3 and 9.4 should address the concept of expired PRA and/or training requirements. Propose changing to read:"...who no longer require such access or no longer meet the training or PRA requirements as specified in R3 or R4..."
22.41	Ameren	Disagree	R9.2, R9.3, and R9.4 - The short period of time to remove access does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that these requirements be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred.

#	Organization	Yes or No	Question 22 Comment
22.42	Black Hills Corporation	Disagree	Recommend that in all cases, network/remote and physical access shall be revoked within 24 hours. All other access shall be revoked within 72 hours. This creates a balance of risk between immediately securing the BES systems and removing "all" access which can become quite intricate.
22.43	ERCOT ISO	Disagree	Recommend: "Each Responsible Entity shall revoke the ability to access its BES Cyber Systems as specified in CIP-011-1 Table R9 - Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Requirements should be revised to address primary and secondary access. Primary access being access to electronic and physical security perimeters (i.e., domain, remote access, badge access). Secondary access being access to assets within the protection of the primary access means (i.e., applications, databases, internal doors within facilities). The timelines listed in 9.1 - 9.4 are acceptable for primary access. Secondary access should allow a more reasonable timeframe. This also needs to address situations where a person may have access to a shared account that would require an outage to change the password. Doing this in a rushed manner would pose a risk to the BES Cyber System and to reliability. Access revocation should be consistent with R5. Recommend SDT consider language addressing access for system administrators and others with high risk access privileges.
22.44	Garland Power and Light	Disagree	Requirement 9.1 - For many companies, it is physically impossible to travel to all substations and change locks within the 24 hour deadline - don't put out a requirement that you know companies cannot comply with - especially for Low and Moderate Impact classified systems.Requirements for 9.1 should be 7 days for Low Impact, 48 hours for medium, and 24 hours high impact location.For requirements 9.3 and 9.4 should the medium impact time requirements should be 7 days.Removing physical access to non-external connected devices (or that only have data output ports connected, i.e. can not be reprogrammed or logged into from that port) should meet the requirements for revoking access for any terminated employee.

#	Organization	Yes or No	Question 22 Comment
22.45	Hydro One	Disagree	Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. We suggest removing requirements 9.3 and 9.4.Requirement 9.1 should be revised to include wording that “terminated for cause” should encompass employees terminated for not only cause, but for suspension or other reasons.
22.46	Northeast Power Coordinating Council	Disagree	Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.Requirement 9.1 should be revised to include wording that “terminated for cause” should encompass employees terminated for not only cause, but for suspension or other reasons.
22.47	Exelon Corporation	Disagree	Requirements 9.2, 9.3 and 9.4 contain time parameters in hours. Exelon’s tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time levels and having a different timeframe for a control center than other locations? Exelon’s position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
22.48	Progress Energy (non-Nuclear)	Disagree	Revoking access within 24 hours will most likely require a special procedure. Revocation of access within a ‘hours’ timeframe implies that the access would be controlled through a security group with 24/7 coverage.Generation subsystems are much less sensitive than any of the control center subsystems. Leave this at 168 hours revocation other than for cause.
22.49	Southern California Edison Company	Disagree	SCE does not feel that reliability is served by imposing a 36 hour revocation for medium impact systems in a control center, and does not see any great distinction

#	Organization	Yes or No	Question 22 Comment
			between medium impact in transmission, generation, or a control center - these should all use a 72 hour timeframe. The timeframe for revocation of access to servers, applications, systems, sensitive information, relays, and equipment, etc. within a physically controlled area should be longer (e.g. 7 days). SCE also requests clarification on what devices must be revoked. The standard does not clarify what immediate revocation of access is - be it access to the "front gate" of an electronic and/or physical boundary versus the revocation of access to each "door" to every system and or component. As such, the potential scope of system access under R9.1 is unclear. SCE Recommends the drafting team revise this so that there is a single requirement for access revocation that and have it sub-divided into sections for physical, electronic, and information artifacts.
22.50	SCE&G	Disagree	SDT needs to consider utilizing the layers of access control leveraged by the exisiting standards here to meet the FERC mandate. Consider allowing entities to revoke access at the firewall level or password level within the timeframes suggested, and then give entites additional time to remove access at all of the other access control layers.
22.51	Florida Municipal Power Agency	Disagree	See comments to Question 19.In 9.2, 9.3 and 9.4 "who no longer require" is an ambiguous term separate from a more defined process of "granting" or "authorizing" access. FMPA suggests: "For personnel who have changed job responsibilities such that authorized access ... is no longer justified".9.3 and 9.4 can be combined into "non-Control Center BES Cyber Systems"
22.52	Liberty Electric Power, LLC	Disagree	See R5 comments on the short times to revoke access. It should be "next business day", not 24 hours in most cases. Further, it should be clear that revoking physical access to an entire facility would serve to revoke physical access to a secure are within the facility.
22.53	Constellation Power	Disagree	Some systems have a single username and password (shared), so when an employee is terminated, is the expectation that every component (such as a similar relay used

#	Organization	Yes or No	Question 22 Comment
	Source Generation		all over the system) have their shared passwords changed? A suggestion would be to allow physical revocation of access in these instances to trump cyber access. R9.4 should state “Generation” with a capital ‘G’ instead of “generation.”
22.54	Entergy	Disagree	Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance point of view to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
22.55	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	The 24 hour requirement of 9.1 will be particularly burdensome for small entities that do not have 24/7 dispatch. While terminations can and should happen after hours when the situation calls for it, those who can revoke access may not necessarily be available. The unintended consequence may be a needed termination being delayed. Another fix would be to increase the number of those able to revoke access, but this may create more problems than it solves.
22.56	San Diego Gas and Electric Co.	Disagree	The access revocation timeframes listed for R9.2 - R9.4 should be consistent, since there is not a significant enough difference in risk between the three requirements warranting different time-periods. R9.4 is contradictory with R9.2 if, by the proposed definition of Control Center, a BES Cyber System controls two or more generation facilities or transmission facilities.SDG&E believes that the requirements in Table R9 should include language clarifying that contractors and service vendors that have access shall have that access revoked (within whatever time frame is appropriate) once the RE is notified by the contactor/service vendor of a contractor/service vendor’s termination. The RE cannot and should not be held responsible for the lack of timely notifications of termination of contractor/service vendor personnel from a contractor/service vendor company. In other words if a contractor were to terminate someone on 1/1/XX and they do not notify the RE until 1/3/XX, the RE should not have to be held to a revocation time period that ends sometime on 1/2/XX.
22.57	Seattle City Light	Disagree	The most mature user provisioning systems with effective processes would unlikely meet the parameters in this requirement. As a result, utilities will modify their

#	Organization	Yes or No	Question 22 Comment
			organizational processes to redefine when "access is no longer needed." For example, rather than submitting a request to remove user access after termination, utilities will await completion of the revocation request before officially terminating employment. This would make the requirement ineffective in accomplishing it's intent.
22.58	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.The requirement should refer to electronic access, not just system access. The 36/72 hour requirement to remove access for routine changes is overly confining, as detailed in the answer to Question 16. Table 5 Part 5.7-5.9 also refer to timeliness of revocation. Twenty-four hours for terminations for cause is reasonable, however having two additional categories complicates matters and could potentially lead to confusion and someone not revoked in the appropriate category. For 5.8, 5.9, 9.2, 9.3 and 9.4, the 36/72 hour requirement to remove access for routine changes is overly confining. We suggest that routine revocation be accomplished within 5 business or 5 calendar days.
22.59	Northeast Utilities	Disagree	The table must be simplified; making a distinction by type of asset only increases risk of non-compliance. For personnel terminated not for cause why not make them all the same?
22.60	FirstEnergy Corporation	Disagree	There is much emphasis in properly categorizing facilities in Attachment II but that information seems to disregarded in information presented in Table 9 of CIP-011. If different timeframes for revoking access is warranted then it should be bases on Low-Medium-High impact - its unclear why a control center and generation/transmission facility is treated differently if each are deemed High Impact. This seems to be an issue in multiple tables dealing with revocation of access privileges - logical and

#	Organization	Yes or No	Question 22 Comment
			physical.Consider replacing 9.2, 9.3 and 9.4 with one row that say 'BES Cyber Systems' with appropriate timeframes for Low, Medium and High impact if needed. However, FE believes the R9.2, R9.3, R9.4, 36 and 72 hours is too restrictive and would like it to remain at the Version 2/3 timeframe of 7 days. To simplify, we recommend consistent revocation of all employees regardless of impact level. In practice most entities will likely implement consistently throughout their organization to the most restrictive requirement. Therefore, not sure the H/M/L levels has a practical use in this situation due to an administrative burden to implement and track differing time periods.
22.61	Powersouth Energy Cooperative	Disagree	This will be greatly affected by the ability to revoke access by account management at the gateway to the cyber system versus the changing of each component that makes up the system. Password/account management on systems such as relays that don't allow individual user accounts will be extremely complicated and time consuming. Consideration should be given to clarifying if managing access at the gateway and revoking physical access is sufficient, especially for low impact systems.
22.62	CWLP Electric Transmission, Distribution and Operations Department	Disagree	Time frames for 9.2 to 9.4 should be extended to 72 hours or next business day, whichever is longer.
22.63	USACE - Omaha Anchor	Disagree	Timelines are unreasonable for removal of electronic access - we do not have 24/7 coverage for revocation of electronic access. Revocation of physical access should be allowed for this section. If they don't have physical access - they can't access the electronic access. Electronic access removal should then be changed to two business days or next business day.
22.64	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 22 Comment
22.65	We Energies	Disagree	We Energies agrees with EEI. It may be appropriate to address revocation of access within the context of "Effective Access." For example, if an individual requires a multi-factor method to access BES Cyber Systems remotely, and one or more of the elements of the multi-factor access is disabled, the individual will not have effective access to the BES Cyber System. Regarding the issue of shared passwords for devices such as relays or PLCs that may exist in hundreds or thousands of locations, if an individual does not have physical access or electronic access to a device, they do not have effective access, even if they have knowledge of a shared password.
22.66	GTC & GSOC	Disagree	We recommend changing this to "36 hours or 1 business day, whichever is greater".
22.67	GE Energy	Disagree	Why introduce a time interval not based on a day? 36 hours may as well be 48 hours.Time periods should be specific to business days and take into account weekends.
22.68	APPA Task Force	Disagree	With physical access control as covered in R5 and remote access control as covered in R13, the greatest risk to the BES is presented by employees and contractors who have been terminated for cause. We therefore recommend the following conforming changes should be made to R9 Table 9.2 - 9.4: R9 Table 9.1: For personnel terminated for cause. Low, Medium and High Impact: "24 hours".APPA recommends elsewhere in these comments that (i) all impact levels have physical access controls in R5 Table 5.1, (ii) requirements in R5 Table 5.7-5.9 be removed, and (iii) requirement R10 Table 10.2 be edited to require passwords to be changed annually, If these comments to the drafting are accepted, the risk of malicious operations is minimal. We therefore recommend the following conforming changes be made to R9 Table 9.2-9.4:R9 Table 9.2: For personnel and others previously granted unescorted access who no longer require such access to Control Center BES Cyber Systems. R9 Table 9.3: For personnel and others previously granted unescorted access who no longer require such access to Transmission BES Cyber Systems. R9 Table 9.4: For personnel and others previously granted unescorted access who no longer require such access to Generation BES

#	Organization	Yes or No	Question 22 Comment
			Cyber Systems.

23. Table R9 provides direction concerning what impact level of BES Cyber Systems to which Requirement R9 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R9 has been moved to CIP-004-5 R6.

Commenters expressed concern that Table R9 is inconsistent with Table R8 for Low Impact BES Cyber Systems, as there should be no requirement to revoke access if there is no requirement to authorize it. In addition, many commenters raised concerns about entities being able to meet proposed revocation times, especially for Low Impact BES Cyber Systems due to the expected large numbers of such systems. The SDT agrees with these concerns, and the requirements for revocation of access for Low Impact BES Cyber Systems have been removed.

#	Organization	Yes or No	Question 23 Comment
23.1	BCTC		Â Recommend collapsing requirements 9.1 to 9.3 into one requirement.Â The time requirements for the one requirement are recommended to be:Â Medium Impact - within 72 hoursÂ High Impact - within 24 hours
23.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
23.3	Florida Municipal Power Agency	Agree	See comments to Questions 19 and 22. Also consider adding “Required for remote access or routable external connectivity only” to Medium and Lower Impact. Lower Impact should be not applicable for 9.1 to be consistent with 5.7. Also, for Medium Impact, 9.1 and 5.7 ought to be consistent.
23.4	Bonneville Power Administration	Agree	The table should refer to electronic access, not system access. The revocation time frames should be adjusted, as discussed above.
23.5	E.ON U.S.	Disagree	: CIP-011-1, R9 has stringent commitments for Low Impact and Medium Impact BES Cyber Systems. E ON U.S. proposes that these time requirements be extended. It is

#	Organization	Yes or No	Question 23 Comment
			not a hard and fast rule as to when employees no longer requires access to 9.4 cyber systems. This is particularly true when an employee is moving to another position within the Company and a certain amount of training is required to backfill their position. Three days does not allow time for that situation. A monthly or quarterly time frame would be adequate in most instances.
23.6	Network & Security Technologies Inc	Disagree	9.1 - Access to Low Impact systems needs to have been explicitly granted (8.1) or at least documented (7.1??) in order to be revoked (consistency issue - also see comments on Question 16).
23.7	Consultant	Disagree	9.1 - If access to Low Impact Systems does not require an authorization process(R8), then it is illogical to require the undocumented access to be revoked.9.1, 9.2, 9.3, & 9.4 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.9.2, 9.3, & 9.4 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.
23.8	Detroit Edison	Disagree	9.1 requires access revocation for Low Impact but there is no requirement to specifically authorize access for Low Impact.
23.9	American Electric Power	Disagree	9.1, Column "Low Impact BES Cyber System", regarding "Within 24 hours". There is no requirement to formally request, authorize, or review access to low impact BES Cyber Systems. How would it be possible to effectively remove that access?
23.10	Constellation Energy Commodities Group Inc.	Disagree	Align time requirement for 9.2 with the other 9.3 and 9.4 (all at 72 hours) to eliminate confusion.
23.11	Oncor Electric Delivery	Disagree	As stated earlier, depending on the type of communication to Cyber Systems, it may

#	Organization	Yes or No	Question 23 Comment
	LLC		not be possible to comply with these requirements due to communication failures. This requirement is particularly burdensome as it applies to contractors and service vendors. Many entities have resorted to weekly verification with their contractors/vendors to verify this requirement. A 24-36 hour requirement, other than "for cause", is not practical.
23.12	Northeast Power Coordinating Council	Disagree	Because the Low Impact levels do not have an access control requirement, Requirement 9.1 is not applicable. Remove the entry from the 9.1/Low Impact BES Cyber System box in the table. Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.13	USACE - Omaha Anchor	Disagree	Believe revocation of physical access should be adequate for this standard - if that were so timelines and impact levels would be acceptable.
23.14	ReliabilityFirst Staff	Disagree	By not specifying a time for revocation of access for low impact assets, the requirement will not be enforceable for these assets. Suggest something like 30 or 90 calendar days for Low Impact BES Cyber System for 9.2, 9.3 and 9.4.
23.15	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
23.16	BGE	Disagree	Combine 9.2, 9.3 & 9.4 revocation for any high impacted system should be consistent. Can the drafting team declare why the time elements were changed from 1 week to 36 or 72 hours?
23.17	The Empire District Electric Company	Disagree	Comments: For item 9.1 through 9.4, we would propose adding the following under Medium Impact: "Required for remote access or routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.For item 9.1, we believe the Low Impact requirement

#	Organization	Yes or No	Question 23 Comment
			should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.18	Exelon Corporation	Disagree	Does this apply to protective relays, even if there is no external access? If so, entities should not have to provide more physical security for a cyber based device or protective relay when it has no external connectivity and therefore would have no more impact to the BES than the other electromechanical devices, protective relays or control switches mounted in the same control panel.Exelon's position is that the access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
23.19	Allegheny Energy Supply	Disagree	Effective Access to low impact systems should be removed within seven calendar days.
23.20	Allegheny Power	Disagree	Effective Access to low impact systems should be removed within seven calendar days.
23.21	San Diego Gas and Electric Co.	Disagree	Even though the compliance timeframes are reasonable in Table R9, two versus three timeframes are preferred. SDG&E believes that the control center timeframe (36 hours) should also be 72 hours, like R9.3 and R9.4.
23.22	USACE HQ	Disagree	First, requirements 9.1, 9.2, 9.3, and 9.4 should be required for every level of impact. Second, to avoid the "Friday 5PM termination with cause" scenario, the language should be change as follow: 9.1, from "within 24 hours" to "Close of Business Day (COB) of the following day after the termination", 9.2 from "within 36 hours" to "Close of Business Day (COB) of the second day after access is no longer required", and 9.3 and 9.4 from "within 72 hours" to "Close of Business Day (COB) of the third day after access is no longer required", OR if requirements 9.2 - 9.4 are collapsed into one requirement (please refer to my answer to previous question) from "within XX

#	Organization	Yes or No	Question 23 Comment
			hours" to "Close of Business Day (COB) of the third day after access is no longer required".
23.23	MRO's NERC Standards Review Subcommittee	Disagree	For item 9.1 through 9.4, we would propose adding the following under Medium Impact: "Required for remote access or routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.For item 9.1, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.24	American Transmission Company	Disagree	For item 9.1, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).
23.25	LCEC	Disagree	I agree with the intent of this requirement but need additional clarification to determine what is meant by revoking system access. Access may be granted at a system or component level. If system, network & wireless access is removed is this requirement satisfied? If audited at the component level, it may not be possible to make all of the necessary changes within the timeframes that are being dictated. The scope of this requirement should be clarified to indicate remote or wireless access only. Component level access will be mitigated by the physical security controls.
23.26	APPA Task Force	Disagree	If our comments in response to Question #22 are accepted, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access). We feel for remote and unmanned BES facilities ensuring and demonstrating compliance with this requirement will be difficult if not impossible to comply with from a logistical standpoint. We also recommend the drafting team allow more time to comply with 9.3 and 9.4. We know there are pressures to have access restricted as soon as

#	Organization	Yes or No	Question 23 Comment
			possible. But there are substantial difficulties in doing so, as many systems have multiple owners, are in remote locations and have numerous devices to access. The drafting team appears to be basing its timetable on a control center environment where the cyber systems are more IT focused and have controls that can be turned on and off easily. We therefore recommend the following changes be made to the impact levels: R9 Table 9.1: Low Impact: For remote access or routable external connectivity only, 24 hoursMedium Impact: For remote access or routable external connectivity only, 24 hoursHigh Impact: 24 hours.R9 Table 9.2: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 36 hoursHigh Impact: 36 hoursR9 Table 9.3: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 1 week.High Impact: Within 1 weekR9 Table 9.4: Low Impact: N/AMedium Impact: For remote access or routable external connectivity only, 1 week.High Impact: Within 1 week
23.27	US Bureau of Reclamation	Disagree	If the requirements of R7 are going to be implemented/established at all levels, the account revocation requirements should be required for the same levels
23.28	Manitoba Hydro	Disagree	Is 24 hours a reasonable and achievable time interval to revoke electronic access to Low Impact BES Cyber Systems? This is too short in consideration of the large number of Low Impact BES Cyber Systems.
23.29	Progress Energy (non-Nuclear)	Disagree	It seems reasonable that access for all impact levels, even low, should be revoked if and whenever it is no longer needed.The complexity and compliance risk of managing all of these requirements at different levels, for different functional areas will be very problematic to substantiate compliance.
23.30	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
23.31	MidAmerican Energy Company	Disagree	MidAmerican Energy does not agree with the timelines specified in Table R9. See the response to question 54.

#	Organization	Yes or No	Question 23 Comment
23.32	Tenaska	Disagree	Most of these are doable on SCADA and EMS hosts only and/or ingress/egress of perimeters/boundaries.10.1 Some DCSes will not allow this for some processes to work.10.2 Same as 10.110.3 must have a way of handling old equipment.10.4 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries .10.5 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.5 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.6 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.7 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.10.8 Should be for SCADA/EMS/DCS hosts only and/or ingress/egress of perimeters/boundaries.
23.33	National Grid	Disagree	o Since the Low Impact does not have an access control requirement, how can Low Impact have Requirement 9.1? National Grid recommends removal of this combination. o The text in 9.2/9.3/9.4 - “who no longer require such access” is vague and should be specific such as transfers, suspensions, or change in job duties.
23.34	American Municipal Power	Disagree	Please provide a little or no impact category
23.35	NextEra Energy Corporate Compliance	Disagree	Please see response to item 22. NextEra believes while it is appropriate to require access revocation requirements for Medium and High Impact BES Cyber Systems, the periods are too restrictive for personnel who transfer, or who separated from the responsible entity via normal means not for cause. NextEra does not believe that 9.1 should apply to Low Impact or No Impact BES Cyber System. In previous section, 8.1 (Authorizing Access) is not required for Low Impact BES Cyber System and the standards should be consistent.
23.36	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management and Table 9 Access Revocation. If account management is not

#	Organization	Yes or No	Question 23 Comment
			required for Low Impact BES Cyber Systems how can account access be revoked within 24 hours? Additionally, if physical security is not required for Low Impact BES Cyber Systems, then Puget Sound Energy suggests including wording similar to Table 5: "Required for routable connectivity only".
23.37	Luminant	Disagree	R9 should not be required for low impact. 9.2 could 36 hours be changed to 48 (2 days) 9.3 and 9.4 1 week
23.38	Ameren	Disagree	R9.1 - Without accounting for who has access this will be a difficult requirement to maintain documentation for Low Impact Systems.
23.39	Black Hills Corporation	Disagree	Recommend that in all cases, network/remote and physical access shall be revoked within 24 hours. All other access shall be revoked within 72 hours. This creates a balance of risk between immediately securing the BES systems and removing "all" access which can become quite intricate.
23.40	Minnesota Power	Disagree	Regarding Part 9.1, Low Impact BES Cyber Systems cannot require revocation, because creation of accounts for these was not tracked in Requirement R8.
23.41	EEI	Disagree	Regarding Table 9 Row 9.1, Effective Access to low impact systems should be removed within 24 hours for the "termination for cause" requirements See question 22 for definition of Effective Access.
23.42	Idaho Power Company	Disagree	Registered Entities will potentially have a large number of low impact systems. One individual may have access to many of the low impact systems. It may not be possible to remove the access from all of them individually within 24 hours.
23.43	Southern Company	Disagree	Removal of access within 24 hours for low-impact systems is unnecessarily burdensome.
23.44	Garland Power and Light	Disagree	Requirement 9.1 - For many companies, it is physically impossible to travel to all

#	Organization	Yes or No	Question 23 Comment
			substations and change locks within the 24 hour deadline - don't put out a requirement that you know companies cannot comply with - especially for Low and Moderate Impact classified systems.Requirements for 9.1 should be 7 days for Low Impact, 48 hours for medium, and 24 hours high impact location.For requirements 9.3 and 9.4 should the medium impact time requirements should be 7 days.Removing physical access to non-external connected devices (or that only have data output ports connected, i.e. can not be reprogrammed or logged into from that port) should meet the requirements for revoking access for any terminated employee.
23.45	Alberta Electric System Operator	Disagree	Revocation criteria should be specified for Low Impact BES Cyber Systems as well. The AESO suggests the following timelines in Table R9:9.1 Low, Medium, and High all Within 24 Hours9.2, 9.3 and 9.4 Low, Within 120 Hours, Medium and High, Within 72 Hours
23.46	Southern California Edison Company	Disagree	SCE does not agree with 36 hour revocation for medium impact systems in a control center, and does not see any great distinction between medium impact in transmission, generation, or a control center. These should all use 72 hour timeframe.Table R9 is that Requirements R9.3 and R9.4 are identical and can be combined. The time constraint for access revocation for low impact system as written is identical across impact levels. This does not reflect the intent of Order 706 where controls are commensurate with impact to BES reliability. The drafting team has selectively interpreted Order 706's directive for "immediate" revocation but has not given adequate consideration to the impact on BES reliability.
23.47	Alliant Energy	Disagree	See response for Question 22.
23.48	ISO New England Inc	Disagree	Since the Low Impact do not have an access control requirement, how can Low Impact have Requirement 9.1? Recommending removal of this combination.Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4

#	Organization	Yes or No	Question 23 Comment
23.49	Northeast Utilities	Disagree	Since the Low Impact does not have an access control requirement, how can Low Impact have Requirement 9.1? Recommend removal of this combination (i.e., Low Impact / For Cause).Requirement 9.2 should use 72 hours for all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.50	Entergy	Disagree	Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance point of view to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
23.51	Southwest Power Pool Regional Entity	Disagree	Termination of access, whether or not for cause, is a basic security control and needs to be applicable to all impact categories.
23.52	The United Illuminating Co	Disagree	The time frames should specify what T=0 is. For example, for termination for cause does the clock start with the termination, or with the notice from Human Resources.
23.53	Dairyland Power Cooperative	Disagree	There should be some time frame for revoking access to low impact systems. 30 days?
23.54	Reliability & Compliance Group	Disagree	They contradict R5.
23.55	FirstEnergy Corporation	Disagree	Timeframes should not be in 'hours' (i.e. less than a full day). Tracking by time rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities. In practice we would likely enforce the most restrictive. As stated in our response to Question 22 the revocation times for a high or medium impact facility should not be different for control centers and other facilities - otherwise why is it "high impact"?Why is Low Impact not covered? This implies a need for a "no impact" category which we believe is warranted.

#	Organization	Yes or No	Question 23 Comment
23.56	ERCOT ISO	Disagree	Timelines should be identified for low impact systems on 9.2, 9.3, and 9.4. The current timeline of 7 days would be appropriate.
23.57	Con Edison of New York	Disagree	Timeliness of access removal is important. This criteria can be interpreted to mean (R9.1 for example) as access needs to be revoked within 24 hours of the actual time of termination for cause. This can be unrealistic. The controlling department, for access, may not be notified by the individuals department of the termination within the time period. This is more likely when contract personnel are considered. The requirement should be clearly worded to provide 24 hours from notification of the termination for cause.
23.58	US Army Corps of Engineers, Omaha Distirc	Disagree	Times will be near impossible to meet for 9.1. Particularly when they cover high medium and low impact systems. Recommend that the emphasis be placed on removing remote electronic access and physical access to facilities. Time frames in terms of business days would be an improvement. 9.1 could be remove remote and physical access by next business day. 9.2 could be remove remote and physical assess within 2 business days. 9.3 & 9.4 within 3 business days. Also have concerns about meaning of "when no longer required" and how this would be tracked and audited. Example would be of an employee that leaves a job but retains system rights in order to train new person.
23.59	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
23.60	Hydro One	Disagree	We believe that changing passwords on non-routable devices isn't realistic and depending on final version of BES CSC list, this may even be unachievable. The standard should allow for other methods of revocation and permit appropriate implementation time.Because the Low Impact levels do not have an access control requirement, Requirement 9.1 is not applicable. Remove the entry from the 9.1/Low Impact BES Cyber System box in the table. Requirement 9.2 should use 72 hours for

#	Organization	Yes or No	Question 23 Comment
			all BES High and Medium Impact Cyber Systems. Remove Requirements 9.3 and 9.4.
23.61	We Energies	Disagree	We Energies agrees with EEI recommendation: Effective Access to low impact systems should be removed within seven calendar days.
23.62	PacifiCorp	Disagree	While we PacifiCorp agrees that terminations for cause require more immediate action to remove access than other terminations; we do not believe that normal terminations and transfers require such timeframes and believe that the current timeframes are more than adequate to ensure the safe operation of the BES. If these timeframes are unavoidable, business days should be considered as opposed to the currently proposed number of hours as this imposes significant risk to our ability todifficulty comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.

24. Requirement R10 of draft CIP-011-1 states "Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 – Account Access Control Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R10? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R10 has been moved to CIP-007-5 R5.

Some commenters expressed concern that password criteria should be provided as guidance, and that entities can increase password strength and meet security requirements without meeting all criteria for password complexity. The drafting team believes that moving all password criteria to guidance would create a significant challenge in auditing this requirement, and would lead to the continued use of Technical Feasibility Exceptions, as entities and auditors may not agree on the most appropriate password policy. However, flexibility in the periodicity of changing passwords has been incorporated in the standards, and the requirement for password complexity was modified to allow more equally effective complexity requirements to be attainable.

Other commenters expressed that Table R10 focuses only on passwords, when there are other mechanisms for authentication (such as tokens). A more flexible requirement has been added to validate credentials before granting access to BES Cyber Systems. This requirement is intended to allow for other types of authenticators.

Some commenters expressed the need to have certain password changes occur during outages, and not necessarily be time based. In response, revisions were made to the password requirements to allow an entity to consider system characteristics when developing a password policy dealing with periodicity of change.

Some commenters suggested combining the requirements R10.6 to R10.8, and they also have concerns about having multiple IDs for different systems and permission levels. In response, the requirement for administrators to have an account for privileged functions was removed because it was too prescriptive. This requirement would not be reasonable to apply on all systems.

Some commenters expressed general concern about being able to enforce the Account Access Control requirements in R10.1 to R10.5. In response, the requirements have been modified to allow for procedural enforcement mechanisms. However, the measure makes clear the challenge in auditing procedural enforcement: entities may be required to divulge their passwords prior to immediately changing them to show compliance.

Some commenters expressed that in R10.7 "explicit authorization" is not defined, and questioned how this differs from R10.8. In response, the term "explicit authorization" has been removed from the requirement. Authorization requirements have been combined

into CIP-004-5, and CIP-003-5 now addresses the delegation of authorization responsibility.. Anywhere authorization is needed in the Standards, the requirement states the authorization occurs by the "CIP Senior Manager or Delegate".

Some commenters requested that the SDT define “privileged” and “other system functions” as used in R10.8. The SDT has removed these terms from the requirements.

#	Organization	Yes or No	Question 24 Comment
24.1	National Rural Electric Cooperative Association (NRECA)		In R10.1, the wording appears to permit changing vendor passwords "anytime" after installation. Do we mean prior to installation or within some specific time after installation. Please clarigy so there is not auditor confusion on what is required here.In R10.7, what what "explicit autorization" mean? Is this different from "authorization?" If yes, please ensure the requirement is clear on what is required.
24.2	WECC		SDT should reevaluate the password complexity requirements as many systems do not support special characters but could still have strong passwords by increasing lengths or changing more frequently. Consider replacing with a requirement that passwords have a minimum bit length (which is what requiring certain lengths, and character sets is prescribing).The password requirements are too weak to be effective. Strong password construction should be required at all levels.
24.3	FEUS	Agree	Agree with comments: The drafting team should clarify when default vendor passwords must be changed after installation (10.1)
24.4	RRI Energy	Agree	Could possibly need a TFE for field installed intelligent electronic devices - meters, monitors, plcs, rtus
24.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Passwords or equivalent should not be so prescriptive and such requirements can result in many TFEs. Also, by creating onerous password requirements, it is more likely to create reliability issues in the BES by having to keep track of complicated passwords; passwords should be both reasonable and functional.The focus of the requirement should be on user accounts. “System”

#	Organization	Yes or No	Question 24 Comment
			accounts should be excluded from many of these requirements (possibly considering new requirements concerning the security of system passwords) to avoid numerous TFEs while maintaining security.User accounts should focus on the password entropy, not on the specifics of number of characters and types of characters. Password entropy is the term used in the computer industry and a much better metric for defining password complexity vs. having to give a specific length or number of characters. For instance, there are 94 ASCII printable characters as described in 10.3, 10.4 and 10.5, so, a 6 character password can have about 36 bits of password entropy. An 8 character password consisting of non-case sensitive alpha-numeric characters (36 characters) has 40 bits of entropy; more than what is described in the standard. FMPA suggests using a metric of 36 bits of entropy for medium-impact password requirements. Such a step will avoid numerous TFEs for older equipment that cannot handle special characters, but can handle longer passwords for instance. FMPA suggests using the NIST's Electronic Authentication Guideline as a baseline for the standard. A copy can be found at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdfA password's information entropy can be expressed by the formula: where N is the number of possible symbols and L is the number of symbols in the password. The function log2 is the base-2 logarithm. H is measured in bits. (See Appendix A in NIST Electronic Authentication Guide referenced above for more detailed information).Even these simple requirements will not pose much of a threat to automated attack which is why these requirements must work together in order to best secure the BES. If securing the BES is the objective, passwords alone are not enough to secure devices; they must be accompanied by logging and alerting systems to ensure industry best practices. For example, a 56-bit password could be cracked in under a day with specialized hardware. A 72-bit password would take over 1,000 years to crack, while 128 bit passwords are currently considered uncrackable by brute force. A 22-character alpha-numeric password has entropy of 128 bits.Footnote 1 is unnecessarily onerous, e.g, if a device cannot support special characters or case sensitivity, but does support 32 character passwords, then the footnote would require use of all 32 characters with around 180 bits of entropy.Also, the focus on passwords

#	Organization	Yes or No	Question 24 Comment
			excludes other, even more secure tools, such as multifactor authentication, that ought to be accounted for.10.1 and 10.2 can be combined “Passwords much be changed upon installation and at least once every twelve months”On bullet 10.6 the wording “the minimum necessary to perform work functions.” is subjective and difficult to measure. We propose this be replaced with “in accordance with the policy required in R1.” In addition, 10.6 is account management and should be in R8, not R10.10.7 is duplicative of 8.1 and should be removed.10.8 is duplicative of requirements in R7 and R8 and should be removed or embedded within that requirement.
24.6	Green Country Energy	Agree	Guidance?
24.7	Emerson Process Management	Agree	In the popular Windows Active Directory, there is no enforcement of complying with password complexity policy. So, the policy can be set for password complexity, the user can still implement weak password without rejection.
24.8	Puget Sound Energy	Agree	Puget Sound Energy suggests including “Where Technically Feasible” to R10, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 10.
24.9	Progress Energy - Nuclear Generation	Agree	R10 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
24.10	National Grid	Agree	Requirements 10.3, 10.4, and 10.5 indicate the “how” which NERC wants to move away from. Suggest moving this to the guidance document.
24.11	US Bureau of Reclamation	Agree	Row 10.4 and 10.5 would be easily reworded into a specific requirement for password construction. Also refer to question #54, comment 2.
24.12	PNGC-Cowtitz-Central	Agree	See comment for question 6.

#	Organization	Yes or No	Question 24 Comment
	Lincoln-Benton-Clallam Group		
24.13	Network & Security Technologies Inc	Agree	Suggestion offered at recent workshop to substitute “ensure authenticity” for “use passwords” has merit and should be considered.
24.14	Alberta Electric System Operator	Agree	The AESO thinks that it is impossible to guarantee a RE can “prevent malicious operation,” however the RE can “mitigate malicious operation.”Please define the term "BES Elements".We agree with the list of criteria that are included in Requirements Table R10.
24.15	Independent Electricity System Operator	Disagree	- R10.2 broaden the scope of passwords and allow for certificates, keys, etc. Some vendors deliver default certificates. In addition, keys may be used for authentication and should be changed. If using two factor or multi factor authentication it techn
24.16	LADWP	Disagree	1. The footnote [1] for CIP-011-1 R10 appears to allow entities to assess TFEs for Account Access Control / Passwords within their own judgment. I would recommend that for 10.3, 10.4, and 10.5 be replaced by footnote [1]. a. The current FERC-Approved TFE process is inefficient; the incorporation of all TFEs into their appropriate requirements should suffice the standard.
24.17	Progress Energy (non-Nuclear)	Disagree	10.1 may be better to indicate ‘upon commissioning’10.7 and 10.8 are too broadly defined to effectively control.It needs to be clarified that it is not required that each device be capable of being configured to automatically enforce authentication requirements (forcing password change, password length, password sophistication, etc.).R10.6 - Recommend clarification of language to indicate that ‘access permission are the minimum necessary to perform work functions’ means normal work functions for each particular individual. There should be no intention to require a single individual to maintain multiple logins for each function for which they are responsible (beyond an administrative login and a ‘normal functions’ login).Consider combining 10.6 and 10.8. If you meet the intent of 10.6 then you should be meeting 10.8.

#	Organization	Yes or No	Question 24 Comment
24.18	LCEC	Disagree	10.1 should be changed passwords prior to production as opposed to after installation.10.1-10.5 lead back to TFE issues. Consider applying only to interactive users.Must address current compliance challenge of requiring technical enforcement of password policies. 10.2 is not auditable as a performance requirement.Footnote [1] is subject to major interpretation: complexity is ambiguous. May not be legally defensible. Maximum should be maximum comparable.We suggest removing 10.6 it is too subjective.
24.19	Idaho Power Company	Disagree	10.1 should specify a period of time after installation or require it before putting it in production. As long as default passwords are changed, low impact systems should have a longer password change cycle
24.20	American Electric Power	Disagree	10.1: Regarding "Change default vendor passwords after installation", suggest using "Default vendor password shall be changed before or during commissioning", or "Change default vendor passwords". The word "after" fails to establish a time frame for the change.10.3: Regarding "Implement a password scheme that has the following attributes:[1]Minimum of six characters", and its footnote. While the footnote potentially allows for some exceptions, this could still be subject to a Technical Feasibility Exception (TFE) process. The TFE process is very cumbersome and provides little value. Based on the direction of CIP-010, the number of TFEs could grow exponentially.10.7: Regarding "Require explicit authorization of access to system and security administrative functions within the BES Cyber System". This seems redundant to 10.6. Would these not be granted based on job function? If not, how is it different than 10.6?10.8: Regarding "Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions". What security benefit does this provide? This defeats any single sign-on functionality. To what level do you limit each account? Why are users required to have more than one account? Will they need more than 2 accounts? What is the limit?

#	Organization	Yes or No	Question 24 Comment
24.21	Dominion Resources Services, Inc.	Disagree	10.8. Some equipment does not support non-privileged accounts. A footnote similar to the one added for 10.3 to eliminate the need for a TFE should be added to 10.8.
24.22	BCTC	Disagree	Â BCTC can see the need for a TFE with requirement 10.2, 10.3, and 10.4Â Requirement 10.7 - we are uncertain as to the objective of this requirement. Does this simply require System Owner, or delegate, approval fro personnel assigned Admin accounts?Requirement 10.8 - we would appreciate some guidance on what type of evidence would be required to demonstrate compliance to this requirement. This seems very difficult to enforce.
24.23	Public Service Enterprise Group companies	Disagree	A rework of the language is needed to address the following questions to avoid confusion and misunderstanding. Please define for 10.7 what is meant by “security administrative functions” and for 10.8 what is meant by “other system functions”. Does the Operating System need automatically to check a user account against a list of “security administrative functions” before allowing access? What needs to be done if the Operating System does not have this capability? Meeting this requirement may not be technically feasible.
24.24	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.Also 10.3 - 10.8 seem to suggest technical authentication enforcement capability for all systems. Suggest softening the language to allow for administrative controls to compensate where technical controls are not possible. Also recommend verbiage that provides consideration for said technical limitations to eliminate the requirement for TFEs.
24.25	FirstEnergy Corporation	Disagree	As written, it appears that this would eliminate many TFEs and we like this change.10.4, 10.5 - Make text in table more generic - ‘implement a password scheme that utilizes as many of the four attributes as possible for the device to which the password applies’. As written, 10.5 would still mean TFE’s for any Microsoft-based authentication systems.Need to provide guidance for 2nd factor authentication (which is typically all numeric) and non-password authentication sources (e.g. smart

#	Organization	Yes or No	Question 24 Comment
			cards)
24.26	Constellation Energy Commodities Group Inc.	Disagree	Choose a single standard for password complexity, rather than differentiating by risk level. Either choose a standard that is compatible with MS Windows, or explicitly state that implementing the maximum password complexity that the device supports is sufficient to meet the requirement without requiring documentation of an exception.
24.27	Liberty Electric Power, LLC	Disagree	CIP-011 R10 changing passwords every 12 months. This is a “feel good” requirement which does not advance security, but rather degrades is as the new passwords are more likely to be written down than the old passwords. The number one method of password theft is reading off a written document.The better method for password security is requiring changes "for cause".
24.28	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
24.29	GTC & GSOC	Disagree	Dictating password attributes requires a specific technology, one that is rapidly becoming obsolete. We recommend the standard should require adequate authentication measures to prevent unauthorized access to systems without specifying passwords as the method for doing so.
24.30	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy is concerned for entities without routable connectivity this requirement is overly burdensome and would require the manual resetting of passwords on thousands of remotely distributed programmable electronic devices. Emergency response would be hampered with the resulting manual password modification and management process. An unintended consequence of not excluding unconnected devices from this requirement may cause an entity to establish connectivity to meet this requirement. This potentially exposes BES cyber system to additional unnecessary security risks which should not be the intention of this requirement. Additionally, password protection may not be available on all BES Cyber

#	Organization	Yes or No	Question 24 Comment
			Systems since some may use other authentication schemes, such as digital certificates or encryption keys. TFEs may be necessary for this requirement.
24.31	Exelon Corporation	Disagree	Exelon is concerned that this will require unique identifiers and passwords for each BES Component despite the ambiguity resulting from the use of the term BES Element which could be read to mean group of components. Exelon suggests that this be limited to only those BES Components which can be remotely accessed via routable or dial-up protocol.
24.32	Constellation Power Source Generation	Disagree	For R10.1, instead of changing passwords "after installation," it should state "upon installation" in case the password is changed before physical installation. R10.2 requires passwords to be changed every 12 months, but in the case of relays for a base loaded generation facility that has planned outages every 3-5 years, this is not possible. The verbiage should add flexibility for planned outages. For R10.4, passwords are not the only way to authenticate, so requiring a password scheme is troublesome.
24.33	Southwest Power Pool Regional Entity	Disagree	Ideally, require user authentication before granting access without prescribing any particular technology. For the requirements specific to password management, add "if used" to the requirement. As written, R10 can be read to mandate the use of passwords. 10.3: Longer is better, especially for administratively privileged accounts. Require 10 or more characters for administratively privileged accounts and at least 8 characters for less-privileged accounts. Where the BES Cyber System Component cannot support the defined length, mandate the maximum password length supported. 10.4 and 10.5: Instead of defining the complexity characteristic, require complex passwords as enforced by the BES Cyber System Component's operating system. 10.7: Define what "explicit authorization" means and clarify if for all types of access or only interactive access. 10.8: Consider rewording the requirement to read "Require users of security administrative accounts to use non-privileged accounts when performing non-administrative functions on BES Cyber Systems."

#	Organization	Yes or No	Question 24 Comment
24.34	Detroit Edison	Disagree	In 10.1 the term “after installation” is vague. Change the sentence to “Change default vendor passwords prior to putting any BES Cyber System Component in service”.In 10.2 change 12 months to “at least once per calendar year, not to exceed 14 months between instances”
24.35	San Diego Gas and Electric Co.	Disagree	In Table R10, Requirement 10.5, SDG&E believes that passwords for high impact systems should be longer, not necessarily more complex. We recommend that high impact system passwords be a minimum of 10 characters. Complexity requirements should be the same for high and medium systems (SDG&E recommends 10.4).Certain legacy devices won’t be able to comply with these password requirements as listed (such as substation serially connected relays), so TFEs may be required for some of these Requirements in CIP-011.The drafting team also may want to consider changing R10 to include other technologies for controlling access besides passwords, such as special locks, biometric devices, etc.
24.36	Hydro One	Disagree	In the case of R10.2 we believe that the change of passwords every 12 months for all three categories would be very difficult to implement and would not provide increased benefit to the overall reliability of the BES. Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.The use of the “minimum” will make 10.6 difficult to audit (refer to the response to Question 54).
24.37	Minnesota Power	Disagree	Is it the Standards Drafting Teams intent that Part 10.7 of Table R10 requires explicit approval for every login to system or security administrative accounts? If yes, Minnesota Power believes that this is excessive and will inhibit proper administration of BES Cyber Systems. Minnesota Power believes that the intent of authorizing access privileges is adequately covered by Requirement R8, subject to the comments made in Question 20.
24.38	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).

#	Organization	Yes or No	Question 24 Comment
24.39	Pacific Gas & Electric Company	Disagree	Need to consider physical security interaction with “cyber” security. An example is a substation control panel (handles, etc, which you can physically operate various devices in a sub) that is physically co-located with electronic devices that perform the same functions. In this case “electronic access control” for local access to should not be required.
24.40	NextEra Energy Corporate Compliance	Disagree	NextEra comments that in reference to the footnote regarding the situation where the "device is not capable of meeting the password threshold, then implement the maximum password complexity that the device can support", isn’t this better presented for the Responsible Entitiy to have a mechanism to file for a TFE or any other exception process proscribed by the Standards?Regarding 10.8, what is the expected documentation and/or account management access control actions to demonstrate requiring users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions?Regarding R10.2, how are BES Cyber Systems not capable of technically enforcing password changes handled? Are procedural controls sufficient to meet this requirement?Additionally, how could one demonstrate compliance with R10.2 if the BES Cyber System Component is not capable of logging when the password was last changed (e.g. protective relays)?Requirement 10.2 time requirement for changing passwords at least once every 12 months does not take into account or include verbiage for legacy systems that do not have the functionality to change passwords, Is there an opportunity for an exception with evidence from the BES Cyber System component manufacturer? There should also be verbiage included in the requirement for exceptions related to BES Cyber system components that passwords cannot be changed due to operational and reliability impacts to the BES. For requirements 10.3 - 10.5, it is unclear how responsible entities document implementing the password scheme requirements. Does the responsible entity comply with having a policy that indicates the necessary requirements or is it necessary that these requirements are enforced technically by the BES Cyber System component? It is recommended that these requirements are satisfied by policies

#	Organization	Yes or No	Question 24 Comment
			instituted by the Responsible Entities and the verbiage indicates that the requirements do not have to be technically enforced. Another recommendation is that there are allowable exceptions to this requirement if a BES Cyber System component cannot technically enforce the requirements, since there are a number of legacy systems that cannot enforce this requirement.For requirement 10.6, there needs to be direction on documenting how access permissions are the minimum necessary to perform work functions. A recommended approach should indicate that the responsible entities administer policies requiring the concept of least privilege concerning their role-based access control administration. Lastly, it is unclear how requirements 10.7 and 10.8 differ from requirement 8.1, since authorization of adding account and subsequent access has to be included in a process based on the requirement. Requirements 10.7 and 10.8 should be moved to 8.X requirements section and clarification should be made as to what explicit authorization means. Is this authorization required each time a user has to access system and security administrative functions? In addition, how is the Responsible Entity supposed to demonstrate compliance to 10.7 and 10.8?
24.41	Southern Company	Disagree	Password requirements written to the level specified in R10.3 through R10.5 have proven unworkable in past versions of the standard. What should be included is only a requirement for strong authentication measures so that alternative, possibly superior, technology is not disallowed.
24.42	Platte River Power Authority	Disagree	Question:Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions What is meant by “other system functions”? What if the “other system functions” require a privileged account?
24.43	Consultant	Disagree	R10 (and others) Suggest the wording "to prevent malicious operation of BES Elements by maintaining control of access to its ES Cyber Systems." be modified to remove the phrase "to maintain control of access to its ES Cyber Systems." Account management and access control do not prevent malicious operation. The objective of

#	Organization	Yes or No	Question 24 Comment
			the standard is to prevent malicious operation, but the requirements control access (in this group), which is only one of the actions required by the standards "to prevent malicious operation."Table R10 - Items 10.3, 10.4, and 10.5 - These are statements of "How To" regarding technical implementation and should be changed to be a "What" requirement by using the words from the footnote: "implement the maximum password complexity that the device can support."Suggest items 10.6 & 10.7 be moved to the table R8, as these statements regard account management rather than access control.Item 10.8 This item should be removed. "Non-privileged account" is not an account type required by R7, and is a subjective term. "other system functions" is not defined and is also a subjective term. "security administrative accounts" is not a defined term. This statement uses multiple undefined and subjective terms and does not establish a requirement that can be implemented or audited.
24.44	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R10. System functionality and capabilities may not allow an entity to meet this requirement. Will there be language added to relieve this requirement if the system is not capable? R10.8 should contain language specifying that it applies to other system functions that do not require system level access.
24.45	Con Edison of New York	Disagree	R10.1 Changing passwords on equipment that are not networked, such as relays, is very labor intense. This activity and will be a year-long job because by the time you finish, you will need to go back to the first relays and start changing those again. The requirement to change these passwords on a yearly basis should be on systems that are networked. There must be a lower level requirement on the non-networked equipment.R10.6 Some system may not technically have the ability to perform this function.R10.8 The purpose of this requirement is not clear.R10.7 requires “explicit” authorization. This requirement should allow for specific personnel designation to be authorized for access and not require it be by name. For example LAN administrators by job definition should be able to be authorized for a specific level of access.R10.8 requires LAN administrators to log in differently if they do not need full access for the current task. This can be enforced procedurally although there should be no expectation that this can be documented to show that in each case the correct login

#	Organization	Yes or No	Question 24 Comment
			was used.R10.8 - Impossible to verify compliance or audit this, should be removed
24.46	Kansas City Power & Light	Disagree	R10.8 is unmanageable in the "windows" world. These requirements are too prescriptive and consideration should be given toward what needs to be accomplished and less on how to accomplish it.
24.47	Western Area Power Administration	Disagree	R10: Biometric and token-based factors not addressed. They need to be. R10.3 - Suggest combining 10.3 & 10.5 to number 10.3 with a 10.3.1 & 10.3.2. R10.4 - Delete 10.4 & just use 10.5 for both Medium & High.R10.4 - Are there exceptions for any equipment that doesn't handle special characters?R10.5 - Are there exceptions for any equipment that doesn't handle special characters?
24.48	ISO New England Inc	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1 and 10.8 repeats 7.2Concerned that 10.6 will be hard to audit, should be a policy statement and included in R1. There is no clear way to audit this requirement and is open to auditor interpretation. This can be easy to audit if an administrator has admin access everywhere or a dispatcher has admin access in the application as well as components. But really an auditor's opinion may differ from BES cyber system's owner.R10.8 Should be a policy statement and included in R1. There is no clear way to audit this requirement. How is this going to be audited? Whether a user has two accounts?R10.7 Please explain "explicit" authorization, versus authorization? They seem to be the same why the emphasis.
24.49	Northeast Power Coordinating Council	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.The use of the "minimum" will make 10.6 difficult to audit (refer to the response to Question 54).
24.50	Black Hills Corporation	Disagree	Recommend that 10.4 be eliminated and medium impact systems be subject to 10.5 (subject to the footnote). Implementing both adds training complexity that has little value.

#	Organization	Yes or No	Question 24 Comment
24.51	Northeast Utilities	Disagree	Regarding 10.4 and 10.5 - Most, if not all, security software can not make the distinction to this level of detail nor can it be effectively monitored manually. Recommend that the criteria MS Windows defines today for password complexity is used. Additionally, trying to make a distinction by BES impact can lead to unnecessary confusion when going to this level of granularity.
24.52	EEI	Disagree	Regarding Table R10 Row 10.1:Default vendor passwords should be changed before or during commissioning for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o “special” characters (e.g. #, $, @, &)Regarding Table R10 Row 10.7:It is not clear what “security administrative functions” means. Moreover, it appears duplicative of requirement 10.6.
24.53	Allegheny Energy Supply	Disagree	Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o “special” characters (e.g. #, $, @, &)This should also include the ability to provide alternatives such as 2 factor authentication where all the types of characters for a single password may not be possible.Regarding Table R10 Row 10.7:It is not clear what “security administrative functions” means. Moreover, it appears duplicative of requirement 10.6.
24.54	Allegheny Power	Disagree	Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o “special” characters (e.g. #, $, @, &)Regarding Table R10 Row 10.7:It is not clear what “security administrative

#	Organization	Yes or No	Question 24 Comment
			functions" means. Moreover, it appears duplicative of requirement 10.6.
24.55	BGE	Disagree	Replace the word "element" with "Cyber System Component" to maintain consistency with the defined terms.
24.56	Duke Energy	Disagree	Requirement 10.1: Passwords should be changed BEFORE making the system operable as opposed to "after installation," as written currently.Requirement 10.2: change passwords once every 12 months. Nuclear plants are on an 18 month fuel cycle. Some are moving to a 24 months. Ideally, systems would be started up at the end of a refueling outage and not touched, save for required maintenance activities until the beginning of the next refueling outage. If the maintenance activity didn't require electronic access, then having each technician/engineer/operator go to the device and change their user specific password on a 12 month basis is actually adding more risk to the BES. Alternate controls can be just as effective with less risk - for instance, installing a stand-alone (e.g. not network/serial/wireless connected) device located in a locked/alarmed cabinet. Is there any allowance for such an alternate control? Also, can this requirement be lessened for low impact systems?10.3 State that multi factor token may be used in place of password.Requirement 10.6: Require that authorized access permissions are the minimum necessary to perform work functions. This applies to user permissions as opposed to administrator functions, correct? Administrator privileges typically include all permissions.
24.57	Nuclear Energy Institute	Disagree	Requirement 10.1: Passwords should be changed before making the system operable as opposed to "after installation," as written currently.Requirement 10.2: change passwords once every 12 months. Frequencies for all requirements should be defined by the Entity, and not defined in these Standards. If a time must be specified in the Standard, then a process must exist for the frequency to be tailored to meet operational requirements.
24.58	USACE HQ	Disagree	Requirement 10.3 should include the language in the footnote to make it clear that

#	Organization	Yes or No	Question 24 Comment
			that is an option under the standard.
24.59	Garland Power and Light	Disagree	Requirement R10 - Paragraph needs to state that a policy or procedure requiring password length, complexity, and password changes are adequate and do not need to be technically enforced by the device.
24.60	Oncor Electric Delivery LLC	Disagree	Requirements 10.5 and 10.7 cannot be applied to all legacy systems currently in-service as they do not support account management. These should allow for TFE. Mandated password change should only be on High impact systems with routable/dial-up communications.
24.61	Xcel Energy	Disagree	Since not all deices are capable of supporting these password requirements, this is an area where TFE need to be allowed. We are concerned with Requirement 10.2 to change passwords every 12 months. For substation devices this would a significant burden, especially for low and medium impact systems.
24.62	ERCOT ISO	Disagree	Since the purpose of this is basically the same as the previous requirements, these could all be combined into a single requirement. 10.1: Recommend specifying a time-frame for changing passwords. 10.2-10.5: Recommend that the requirements address the use of alternate authentication means, such as biometrics and RSA SecurID. TFEs should be allowed for the requirements under this section.
24.63	MidAmerican Energy Company	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
24.64	Ameren	Disagree	Suggest changing R10.1, R10.2, and R10.3 for Low Impact BES Cyber System requirement to “Required, unless system is behind a firewall or other protective measures.” Giving password strength criteria is too specific when entities may use

#	Organization	Yes or No	Question 24 Comment
			other ways to implement security that meet or exceed this requirement. The manpower necessity for changing passwords yearly and maintaining a protected/immediately accessible database to store passwords so that those who need to access relays can when needed for Low Impact Systems is not needed. If all the High Impact System relays have firewall protection that should be enough. The industry needs to be able to access relays to keep the BES system functional and respond to operational issues. Also, for R10.1 need to clarify how long after installation should a vendor password be changed.â€,â€,R10.4 and R10.5 - These requirements will be difficult to prove in an audit. Should be changed to provide a documented process should be sufficient and should be less trouble in dealing with an audit on these requirements. However, some systems may not be able to adhere to these policies, and TFE's may be required.R10.6 - Documentation of the permission check will be volumes of data that will have to be performed in the audit. This requirement needs a periodic review time associated with it.R10.7 - What is the intention of this requirement? If all access is already accounted for in R10.6 isn't this requirement duplicate effort?
24.65	Entergy	Disagree	Suggest simplifying requirements 10.4 and 10.5 by combining and rewriting into: “Implement a password scheme that cannot be found in the dictionary and has at least three of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, “special” characters (e.g. #, $, @, &)”Requirement 10.8 should be reviewed from a technology perspective. While use of a “normal” user account and gaining “root” access through “sudo” is robust in the UNIX variant operating systems, performing the same function in the Windows operating system can be problematic with logging in as a different user all together. Suggest possibly relaxing this requirement.
24.66	ReliabilityFirst Staff	Disagree	Table R10; row 10.2 - High Impact BES Cyber Systems should have the password changed at least every 6 months. Regarding footnote 1, for devices that are not capable of meeting the password threshold, the entity should be required to

#	Organization	Yes or No	Question 24 Comment
			document this situation, including compensating measures, for audit review.
24.67	Southern California Edison Company	Disagree	Technical capability is not a homogenous quantity in a system with diverse classes of devices and thus the ability to implement generic controls over a heterogeneous system does not always exist. A means to seek exception from the "word" of the standard, while still complying with the intent which is to clearly identify technical situations where a prescribed control, is not implementable while maintaining cyber security protections is needed. Requirements R10.4 and R10.5 are too prescriptive and do not allow registered entities to seek out alternative access authentication mechanisms. For instance, biometrics or 2-factor authentication based on numerical passwords generated by a key-based security architecture may not meet the word of the standard but go above and beyond the intent of the standard.
24.68	USACE - Omaha Anchor	Disagree	TFE will be required for this section if verbiage isn't added to address lower level machines where some items (10.7, 10.5) are not possible.
24.69	Manitoba Hydro	Disagree	The account access control requirements should be more generic and technology independent, allowing the entity to apply a variety of account access controls. If passwords are needed, Requirement R10.3 should also require some "special" characters, to the extent that the device is capable. The standard should also allow protection by layers of security, which may be provided by other methods or cyber systems.
24.70	APPA Task Force	Disagree	The APPA Task Force supports the proposal by MRO-NSRS to be more generic in the wording of the requirements in R10, to account for innovations such as biometric controls used in lieu or in conjunction with password controls.We propose the following edits to R10:R10 Table 10.1: Restrict electronic access to BES Cyber Systems through use of an electronic access control that does not use/rely on the vendor defaut password.R10 Table 10.2: Electronic access controls must be updated/modified at least once annually.Since numerous devices would be exempt from this requirement due to their inability to support password protection, the term

#	Organization	Yes or No	Question 24 Comment
			"Electronic Access Controls" should replace "Passwords". This is non-limiting and will not lock into the standard a current technology, for example, keyboard-based "password access."APPA proposes that items 10.3 - 10.5 be removed from this requirement and be submitted to the "guideline in support of the standard" drafting team to be included as a best practice for account access control. If 10.3-10.5 must remain in the requirement we recommend they be less technology-specific. We propose the following language:R10 Table 10.3: Implement a password scheme that has a minimum of six characters, or an electronic access control with an equivalent or superior technology option.R10 Table 10.4: Implement a password scheme that has at least two of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, "special" characters (e.g. #, $, @, &), or an electronic access control with an equivalent or superior technology option. R10 Table 10.5: Implement a password scheme that has at least three of the following four attributes: Lower case alphabetic, upper case alphabetic, numeric, "special" characters (e.g. #, $, @, &), or an electronic access control with an equivalent or superior technology option.In Table 10.6 the wording "the minimum necessary to perform work functions" is subjective and will be difficult to measure. We propose this be replaced with "Require that access permissions are in accordance with the entity access authorization policy required in R1."
24.71	Constellation Energy Control and Dispatch, LLC	Disagree	The appropraite account access control mechanisms should not be specifically defined in the Table R10.
24.72	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In today's electronic world there are many methodologies for electronic access control. Many systems now make use of multi-factor passwords, and/or biometrics. They use passwords or

#	Organization	Yes or No	Question 24 Comment
			pass-codes are randomly generated, encrypted and time sensitive. Access codes or passwords may be one time, expiring after one use, and/or after a specified time (usually 60 seconds). The systems implemented may also provide checks to insure that the passwords are not captured and hijacked. These modern methodologies are far more effective and secure than the stated requirements. This requirement is prescriptive and too specific. The way it is written it would preclude the use of modern and stronger tools because they may technically not meet one or more of the specifications, even though they are bigger, better and stronger. If the requirements must remain this prescriptive, then the following changes should be made:- There should be a second footnote, "Stronger methods, such as multi-factor authentication of one-time passwords, may be used in lieu of username/password combinations."- 10.1: A time frame for "after installation" needs to be specified.- 10.3: Given the efficacy and availability of Rainbow Tables, a 6-character password is woefully inadequate. The minimum should be at least 10, and 14 would be better. - 10.6: There's a difference between "minimum necessary" and "minimum practical and necessary". Strict interpretation would require that access grants would change depending on the task being performed, which is probably not the intent. Suggest the wording be changed as described. An alternative would be to use the NIST definition of "Least Privileges - The security objective of granting users only those accesses they need to perform their official duties" (NIST IR 7298 - NIST Glossary of Key Information Security Terms) and then require the use of Least Privileges.Item 10.2 in Table R10 states that “/p/asswords must be changed at least once every 12 months”. Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently passwords must be changed.
24.73	Reliability & Compliance Group	Disagree	This requirement does not consider the use of biometric access systems such as finger print readers that could be used in place of password verification.Also, it should include the word “electronic” when it talks about “maintaining control of access to its BES Cyber Systems.”

#	Organization	Yes or No	Question 24 Comment
24.74	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding footnote 1 and Table R10 Row 10.7.
24.75	American Transmission Company	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12 months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.We would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here. Finally, the standard should allow for other control methods such as front ending a device with a fully password protected access control device instead of the required password controls directly on the device.
24.76	MRO's NERC Standards Review Subcommittee	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12

#	Organization	Yes or No	Question 24 Comment
			months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.Finally, we would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here.
24.77	The Empire District Electric Company	Disagree	We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12 months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.Finally, we would propose deleting items 10.3 - 10.5, as they would not apply under the approach proposed here.
24.78	We Energies	Disagree	We Energies agrees with EEI: Regarding Table R10 Row 10.1:Where possible, default vendor passwords should be changed before being commissioned for use.We Energies agrees with EEI: Regarding footnote 1, change to: If a device is not capable of meeting the password threshold, then implement as many of the following password attributes as possible: o Minimum of six characters o Lower case alphabetic, o upper case alphabetic, o numeric, o "special" characters (e.g. #, $, @, &)We Energies agrees with EEI: Regarding Table R10 Row 10.7:It is not clear what "security administrative functions" means. Moreover, it appears duplicative of requirement 10.6.

#	Organization	Yes or No	Question 24 Comment
24.79	PacifiCorp	Disagree	While the criteria themselves are not onerous for the long term/future development of the systems, the fact is that current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.The standard needs to allow for non-password based authentication systems or one time passwords. Modify 10.2 through 10.5 with “or equivalent or greater authentication methods”The current password requirements in table 10 are too burdensome and unnecessary. The requirements as written are also confusing. Passwords should not be the only acceptable way to authenticate a user prior to granting access.
24.80	Luminant	Disagree	Will require TFE for some systems

25. Table R10 provides direction concerning what impact level of BES Cyber Systems to which Requirement R10 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R10 moved to CIP-007-5 – Cyber Security - Systems Security Management - Requirement R5.

Commenters indicated that passwords on Low Impact BES Cyber Systems should not be subject to any periodic change as stated in Table R10 (10.2). In response, the SDT revised the password requirements, and they are not applicable for Low Impact BES Cyber Systems.

Commenters suggested a single criterion for password complexity. In other words, do not differentiate by risk level. The SDT agreed and reduced the password complexity requirement to be the same regardless of applicable risk or impact level.

#	Organization	Yes or No	Question 25 Comment
25.1	US Army Corps of Engineers	Agree	Agree with impact levels, but disagree on item Table R10, 10.8: "Require users of BES Cyber Systems and security administrative accounts to use non-privileged accounts when accessing other system functions." Add to the end of the statement, if the system function does not require the use of using a privileged account.
25.2	CWLP Electric Transmission, Distribution and Operations Department	Agree	As long as TFEs are available for systems that do not support the password requirements.
25.3	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
25.4	US Bureau of Reclamation	Agree	Recommend we establish Requirement 10.6 for all impact levels. Also, please refer to question #54, comment 2
25.5	Southern California	Agree	Requirement 10.7 may be interpreted that access need not be denied as a default

#	Organization	Yes or No	Question 25 Comment
	Edison Company		setting. If the intent of the drafting team is a different control, the team should consider rephrasing this requirement.
25.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
25.7	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels for R10 if it is understood that a blank in the table means N/A. The APPA Task Force agrees with the MRO-NSRS proposal:"If the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems."
25.8	GTC & GSOC	Agree	We recommend 10.8 to be changed to: "Require persons to use non-privileged accounts when accessing system functions that do not require privileged accounts"
25.9	Exelon Corporation	Agree	We would suggest the password items begin with "Where passwords are utilized they must ...." These requirements should allow entities the flexibility to use other user authentication methods besides just passwords such as two factor tokens or other methods that provide even better protection than just passwords. Exelon appreciates the clarification provided in footnote #1 which has the potential to limit the number of TFEs that would be required.
25.10	Regulatory Compliance	Disagree	10.1 - 10.3 STRIKE "Required" for Low Impact10.6 - STRIKE "Required for medium impact - inconsistent with level.
25.11	LCEC	Disagree	10.2 is not auditable as a performance requirement.Footnote [1] is subject to major interpretation: complexity is ambiguous. May not be legally defensible. Maximum should be maximum comparable.We suggest removing 10.6 it is too subjective.
25.12	BGE	Disagree	10.2 maintain consistency for timeframes (i.e. use 12 months or annual). 10.3, 10.4

#	Organization	Yes or No	Question 25 Comment
			and 10.5 should be combined.10.6 needs a definition for “minimum”. 10.8 needs clarification for the meaning of “other system functions”.
25.13	Dominion Resources Services, Inc.	Disagree	10.2. It is anticipated that there will be thousands of Low Impact devices geographically spread across a utility’s system. By definition these devices provide little risk to the BES. It is impractical from a resource perspective and unnecessary from a reliability perspective to change the passwords of low impact components every 12 months. The requirement should be removed from Low Impact.
25.14	ERCOT ISO	Disagree	10.7-10.8: Should apply to Medium Impact BES Cyber System.
25.15	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
25.16	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. For example, a reasonable estimate is that our Entity will have approximately 2,500 low-impact substations with an estimated 100 programmable devices in scope per substation. Without any other consideration of work required, that represents 250,000 password changes each year to be performed, tracked, and communicated. The majority of those devices have hardware override switches which disable password protection for anyone who has physical access to the device, so no reliability advantage is gained by performing the password change. This is just one example of the scope of work with little or no benefit to the BES that is required as long as there are per-component low-impact requirements.The standards should be modified so that requirements for low-impact cyber systems include only program-wide efforts such as policy, governance, incident response planning, and disaster recovery planning.If low-impact requirements cannot be eliminated completely, then at least the specific requirements for password changes for components with no external connectivity should be removed, as they provide no additional benefit when paired with physical security requirements.In addition, vendor contracts with sole suppliers of necessary equipment may conflict

#	Organization	Yes or No	Question 25 Comment
			with 10.1. At the least, this creates the necessity for a large, cumbersome TFE program.In 10.1, the phrase "after installation" should be replaced by "before, during, or immediately after installation".10.4 and 10.5 create a TFE burden without any substantial benefit and disallow advanced technology that provides stronger authentication but does not meet the literal wording. Instead, the requirement should be modified to require authentication.
25.17	Tenaska	Disagree	At the end of R11 just add "identify restrictions and uses for accesses". And remove table.
25.18	Constellation Energy Commodities Group Inc.	Disagree	Choose a single standard for password complexity, rather than differentiating by risk level.
25.19	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
25.20	The Empire District Electric Company	Disagree	Comments: With the changes proposed in question 24, we would propose that revised items 10.1 and 10.2 be "Required" for Low, Medium, and High Impacts.We would agree with the current impact levels for items 10.6 - 10.8.However, it the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems. Once someone has gained physical access to a facility, the hurdle of a password does very little to limit the amount of physical damage or misuse that can be done. However, for remote access, the password becomes critical to preventing damage or misuse. We also believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
25.21	Southwest Power Pool	Disagree	Complex passwords and minimum password lengths are a basic security control and

#	Organization	Yes or No	Question 25 Comment
	Regional Entity		should be applicable to all impact categories.
25.22	E.ON U.S.	Disagree	E.ON U.S. does not believe a requirement is necessary for low impact items.
25.23	Consultant	Disagree	Item 10.2 - There is no requirement for account management for Low Impact assets, and it is illogical to require password controls where there are no account controls.
25.24	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
25.25	Progress Energy (non-Nuclear)	Disagree	Low impact BES systems should not have this requirement. By virtue of their definition they do not need this requirement.CIP-011 R10 - Would like to compliment the SDT for constructing a realistic and reasonable approach with regard to effective use of complex passwords. The SDT has recognized that there may be password complexity limitations with older existing electronic gear that is in operational service and rather than try to mandate a standard that is technically not feasible to implement, they have provided the footnote to require that practical password complexity should be set to the maximum that the device is capable of supporting.CIP-011 R10 - Account management access control & passwords is this meant to include BIOS or only interactive logins to devices?10.2 - “Passwords must be changed at least once every 12 months”, If this is referring to cyber system components, this represents unreasonable costs to utilities. Password changes for relays with no remote capability will be cost prohibitive, and password changes for individual relays with remote capability will require excessive time.
25.26	NextEra Energy Corporate Compliance	Disagree	NextEra believes for Low Impact BES Cyber Systems, requiring passwords to be changed at least once every 12 months should be changed at least every 24 months; for Medium Impact BES Cyber Systems, we suggest changing passwordsat least every eighteen months.
25.27	Alberta Electric System	Disagree	Please consider the following changes to increase security and make the

#	Organization	Yes or No	Question 25 Comment
	Operator		requirements more restrictive:Table 10.2 - passwords changes at least once every three months.Table 10.3 - minimum eight character password (with same footnote)Table 10.4 - change to “three of the following five attributes” and include two-factor authentication as an additional attribute.Table 10.5 - change to “four of the following five attributes” and include two-factor authentication as an additional attribute.Table 10.6 - required for Low, Medium, and High impact levelsTable 10.7 - required for Medium and High impact levelsTable 10.8 - required for Medium and High impact levels
25.28	American Municipal Power	Disagree	Please provide a little or no impact category
25.29	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 7 account identification to Table 8 account management, Table 9 Access Revocation, and Table 10 Account Access Controls. Additionally, if physical security is not required for Low Impact BES Cyber Systems, then Puget Sound Energy suggests including wording similar to Table 5: “Required for routable connectivity only”.
25.30	Con Edison of New York	Disagree	R10.6 should not be required for medium impact
25.31	Ameren	Disagree	R10.8 - Should be added for Medium Impact Systems.
25.32	ISO New England Inc	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1 and 10.8 repeats 7.2
25.33	Hydro One	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.We’d like to know the full meaning of “explicit authorization”. If possible please add the definition in the glossary.
25.34	Northeast Power Coordinating Council	Disagree	Recommend removing 10.7 and 10.8 since these are covered by 8.1, and 10.8 repeats 7.2.

#	Organization	Yes or No	Question 25 Comment
25.35	Black Hills Corporation	Disagree	Recommend that 10.4 be eliminated and medium impact systems be subject to 10.5 (subject to the footnote). Implementing both adds training complexity that has little value. Similarly, 10.7 & 10.8 should also apply to medium impact systems.
25.36	Northeast Utilities	Disagree	Recommend that the 10.4 scheme (use 2 of 4) is used for both medium and high impact and that the 10.5 scheme (use 3 of 4) is eliminated. Trying to make a distinction by BES impact can lead to unnecessary confusion when going to this level of granularity.
25.37	Minnesota Power	Disagree	Regarding Part 10.2, Minnesota Power believes that the requirement to change passwords for Low Impact Systems at least once every 12 months is excessive. The requirement that a Registered Entity change passwords within this time frame for all BES Cyber Systems is unnecessarily cumbersome and time consuming. In addition, the coordination that would go into making these changes is infeasible and could result in an inability to access the system. In addition, Minnesota Power recommends that the Standards Drafting Team consider adding the following qualifier to Parts 10.1 through 10.5 of Table R10:"...where passwords are used for access control."
25.38	MidAmerican Energy Company	Disagree	Requirement 10.1 needs to state “Change default passwords prior to production operation” or words to that effect. It is imperative that vendor passwords are never placed into a production environment.
25.39	PacifiCorp	Disagree	Requirement 10.1 needs to state “Change default passwords prior to production operation” or words to that effect. It is imperative that vendor passwords are never placed into a production environment.
25.40	SCE&G	Disagree	SDT should consider not requiring Low Imapct systems to have passwords changed annually. This could potentially generate a high volume of TFEs for hardcoded passwords as previously described.

#	Organization	Yes or No	Question 25 Comment
25.41	Constellation Energy Control and Dispatch, LLC	Disagree	See comment provided to question 24
25.42	LADWP	Disagree	See previous
25.43	Western Area Power Administration	Disagree	See previous
25.44	WECC	Disagree	Several of the actions should be done for low impact assets, such as “Require that authorized access permissions are the minimum necessary to perform work functions”. Consider relooking at the impact levels.The password requirements should apply to all impact levels.
25.45	Allegheny Energy Supply	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.46	Allegheny Power	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.47	EEI	Disagree	Sufficient Password security can be accomplished by combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.If low-impact requirements cannot be eliminated completely, then at least the specific requirements for password changes for

#	Organization	Yes or No	Question 25 Comment
			components with no external connectivity should be removed, as they provide no additional benefit when paired with physical security requirements.
25.48	Duke Energy	Disagree	Table 10: o All of Table 10 will potentially require a TFE o 10.1 change 'after installation' to "prior to being placed in service" o Suggest all password verbiage be replaced with 'authentication method' and remove specified attributes. Otherwise TFEs will be required for 10.3-10.5. o For 10.2 change 'at least every 12 months' to 'when security conditions require' o Requirement 10.2: Can this requirement be lessened for low impact systems? o 10.8 requires multiple accounts for individuals with admin rights on individual accounts. Suggest making this applicable only for shared admin accounts or removing for Windows based systems.
25.49	ReliabilityFirst Staff	Disagree	Table R10; rows 10.7 and 10.8, should be "required" for medium Impact BES Cyber Systems.
25.50	Dairyland Power Cooperative	Disagree	The focus is entirely on passwords, but other forms of credentials can be used. For example there are certificate or key based authentication to many systems. Many vendors use default keys that need to be changed, just as default passwords. The password rules are very weak compared to common practices. This seems to be an attempt to encourage the strongest possible password on legacy components/systems, but the by-product is that this weakens the requirements for modern systems. There should be a better way to deal with legacy systems while requiring new systems to use stronger passwords.
25.51	FirstEnergy Corporation	Disagree	The impact levels are agreeable assuming the changes suggested in Q24.10.1 Vendor default passwords should be changed based upon a clear definition of "installation." Non-password authentication sources need to be addressed. Possibly combine 10.4 and 10.5, but keep the note on implementing the maximum password complexity.FE request that the "Required" shown in the Low Impact column of rows 10.2 and 10.3 be removed. Password changes to Low Impact items should not be a requirement in the standard but left as a "best practice" guideline. A requirement to annually change

#	Organization	Yes or No	Question 25 Comment
			passwords to multiple digital protection relays associated with Low Impact facilities would be extremely burdensome with little reliability improvement. Each relay would require individual attention as there is no method of globally changing all digital relay passwords. If retained, consider allowing entities to synch up the changing of passwords on these devices with their normal PRC-005 maintenance cycles.
25.52	Southwestern Power Administration	Disagree	The language in this requirement should be changed to include a broader scope of technology or to be technologically neutral so that new or emerging technology (such as biometrics) which may be more secure than passwords will still be considered as in compliance.
25.53	Entergy	Disagree	The requirement indicates that the drafting team believes protection of sensitive information associated with allegedly “low impact” BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.Suggest making password requirements for all assets meet the requirements for high assets and let foot note as written take care of the assets that are unable to meet the requirement.
25.54	American Transmission Company	Disagree	The standard should allow for other control methods such as front ending a device with a fully password protected access control device instead of the required password controls directly on the device.
25.55	Florida Municipal Power Agency	Disagree	The table should have different levels of password entropy required for the different impact areas. For example, medium impact systems should have 40-bits of required entropy, while high impact systems should require 64-bits of entropy. Low impact may be able to get by with 32-bits of entropy.
25.56	Oncor Electric Delivery LLC	Disagree	These requirements should only apply to Control Center Cyber Systems.
25.57	We Energies	Disagree	We Energies agrees with EEI: Sufficient Password security can be accomplished by

#	Organization	Yes or No	Question 25 Comment
			combining table items 10.1 through 10.5 into one line item. The item should state: Implement a process for authenticating all users prior to granting access to BES Cyber Systems. If additional security measures are desired for high impact BES Cyber Systems require dual authentication when possible.
25.58	MRO's NERC Standards Review Subcommittee	Disagree	With the changes proposed in question 24, we would propose that revised items 10.1 and 10.2 be "Required" for Low, Medium, and High Impacts.We would agree with the current impact levels for items 10.6 - 10.8.However, if the standard were to remain as written, we would propose that the 10.1 - 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems. Once someone has gained physical access to a facility, the hurdle of a password does very little to limit the amount of physical damage or misuse that can be done. However, for remote access, the password becomes critical to preventing damage or misuse. We also believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
25.59	Emerson Process Management	Disagree	With the latest Windows OS, there is really no great difficulty of asking for complex password. This requirement can be easily applied. The only thing is enforcement. This enforcement may be retuired for high or medium impact BES Cyber Systems.

26. Requirement R11 of draft CIP-011-1 states "Each Responsible Entity that allows remote or wireless electronic access to any of its BES Cyber Systems shall apply the criteria specified in CIP-011-1 Table R11– Wireless and Remote Electronic Access Documentation to ensure that no unauthorized access is allowed to its BES Cyber Systems. Do you agree with the list of criteria that are included in Requirements Table R11? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

The remote access requirements from CIP-011-1 have been moved to CIP-005-5 - Cyber Security - Electrnic Security Perimeters – Requirement R2. The wireless requirements have been removed.

Commenters suggested more clarity was needed in the terms "remote access" and "external connections" and "wireless". The SDT proposed the following formal definitions for additional clarity on "remote access" and "external connectivity," and removed wireless access requirements from the revised Standard.

External Connectivity: *Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter*.

External Routable Connectivity: *The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.*

Interactive Remote Access: *Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.*

Commenters suggested that wireless and remote access be broken out into separate requirements. In response, the SDT notes that wireless access requirements have been removed from the Standard. There is a single requirement for Remote Access in CIP-005-5 R2.

Commenters stated that given the local definition of Remote Access, the requirements of Table 11 Row 11.2 are extremely unclear. In response, a new requirement for Remote Access Management (CIP-005-5 R2) was created based on the Urgent Action Revisions to CIP-005-3.

#	Organization	Yes or No	Question 26 Comment
26.1	Regulatory Compliance	Agree	BUT:11.1 Please clarify whether these are wireless technologies within the electronic boundary or wireless technologies originating outside the electronic boundary.
26.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
26.3	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made."shall implement the requirements ..." makes the bullets individual requirements, which FMPA does not believe what the intent of the drafting team. FMPA suggests "shall implement the security controls ..." as an alternative.Consider combining R7, R8, R11 and R12. FMPA believes the standard should be more clear as to if this is wireless connection that is under the complete control (end-to-end) of the Responsible Entity or not. There is no way an individual can ensure that their data path, once outside of their control, routes over a wireless device or not. For access that is not under the control of the RE, the standard should refer to it just as it might for any other remote access control, demanding that the data is encrypted and the end point is protected.
26.4	Progress Energy - Nuclear Generation	Agree	R11 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
26.5	BCTC	Agree	Suggest rewording from Wireless and Remote Electronic Access to Wireless or Remote Electronic Access
26.6	APPA Task Force	Agree	The APPA Task Force believes disabling the wireless functionality should be an option. If the description is not changed as proposed in Question #17 then we recommend that R11 Table 11.1 should include "and/or document that the wireless functionality is disabled."

#	Organization	Yes or No	Question 26 Comment
26.7	Bonneville Power Administration	Agree	The objective of this requirement ("to ensure that no unauthorized access is allowed to its BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.It it not clear that wireless needs to be specifically addressed. It is one of many access methods that may be use. If it is to be specifically addressed, then it should be treated separately, but as a sub-class of remote access. (Even if wireless access is intended to be used for access by Entity personnel, its very nature means that access could be gained from other locations.)If it is addressed at all it should be limited to requiring adequate protection for Wireless Access Points, but not to the level of specifically prescribing the methods that need to be taken.Finally, "Wireless Access" needs to be defined. The most common usage refers to wireless local area networks under one of the 802.11 standards. But, technologies such as point-to-point communications using microwave or laser are also wireless technologies. We offer no suggestions for the definition, since we do not know the intent of the team.
26.8	Progress Energy (non-Nuclear)	Agree	We like the clarity provided by the use of the term "interactive" remote access.
26.9	Independent Electricity System Operator	Disagree	- R11 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.- R11.1 - Is this just a policy stat
26.10	BGE	Disagree	11.1 Define "wireless technology" (i.e. could implicate a cell phone). Throughout the table when "external connectivity only" is stated this can be interpreted as a connection from the DMZ or other company network.
26.11	Black Hills Corporation	Disagree	All BES systems should have should have access controls regardless of hard line /

#	Organization	Yes or No	Question 26 Comment
			remote / wireless connection.
26.12	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protction and type of access granted.
26.13	Southwest Power Pool Regional Entity	Disagree	An important aspect of wireless access was overlooked. Prescribe the use of available security features on all wireless access points. If possible word the requirement to not prescribe specific characteristics of configurations (WEP versus WPA, SSID broadcast, MAC address filtering, etc.) in order to not preclude next generation technology.
26.14	Southern Company	Disagree	Better specificity is needed as to what constitutes wireless access. Is the intent limited to 802.11x access or is the intent to include all communication done without wired connectivity?R11.1 This requirement could be interpreted to include all wireless, including voice. Insert “network” prior to “technologies”.
26.15	Luminant	Disagree	Combine 11 and 12? Does this apply to a remote user that may be connected via a wireless network connection at a remote location?
26.16	CenterPoint Energy	Disagree	Disagree - For R11.1, CenterPoint Energy is not clear as to what is meant by "use restrictions". Table R11 is titled "Wireless AND Remote Electronic Assess..." but R11 states "Each Responsible Entity that allows remote OR wireless electronic access..." CenterPoint Energy suggests separating remote and wireless access requirements. CenterPoint Energy also suggests adding clarification as to type of wireless protocols that should be included.
26.17	Exelon Corporation	Disagree	Exelon feels that definition of access needs clarity. Is this meant to include “view only” access or is it limited to administrative access that allows for maintenance, trouble shooting or modification of BES Cyber Systems?
26.18	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote

#	Organization	Yes or No	Question 26 Comment
			connectivity (R11, R12, R13) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Same for R13.Distinction between "remote access" and "external connectivity" is not clear. More clear definitions may need to be provided. Such as, external connectivity allows for direct Internet access vs. remote connectivity allows for access from the enterprise WAN.Table 11: suggest removing 11.3 for low impact systems. No need to authorize remote access when physical or electronic access is not authorized.
26.19	Allegheny Energy Supply	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.20	Allegheny Power	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.21	EEI	Disagree	Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.22	Constellation Power Source Generation	Disagree	In general, Constellation Power Generation believes that wireless controls should be combined with network controls, as the same controls will be applied.
26.23	Minnesota Power	Disagree	In reading and applying the definitions of "remote access" and "external connectivity," remote access is a specific type of external connectivity. Therefore, any reference to criteria for remote access based on whether or not it is externally connected is redundant. In addition, by definition all wireless access is also remote access and this should be stated or otherwise clarified.Regarding Part 11.3 of Table

#	Organization	Yes or No	Question 26 Comment
			R11, does this require explicit approval for every remote login to BES Cyber System accounts? If yes, Minnesota Power believes that this is excessive and will inhibit proper administration of BES Cyber Systems. Minnesota Power recommends changing the language to clarify that Part 11.3 requires that a Registered Entity determine who has authorized remote access privileges.
26.24	Southwestern Power Administration	Disagree	Is a separate requirement for wireless access really necessary when a requirement already exists for protecting access to a BES Cyber System by any means of entry? If so, then suggest separating wireless from remote access.
26.25	Dairyland Power Cooperative	Disagree	It is unclear if the standard wants to make a distinction between wireless and remote access, or an equivalence.
26.26	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with SPP's observation below:We question the need for a specific requirement for wireless devices. We understand there have been inquiries about treatment of wireless devices. But a wireless access point has the same impact on a BES Cyber System as any other access point. A requirement to protect access to a Cyber System already includes any possible means of entry. The use of a wireless device to access a BES Cyber System can be determined with an audit of access logs and a further audit of control of that access would reveal whether appropriate protections were in place. There is not a need for a separate distinct requirement subject to records retention and audit for specific wireless devices. NERC must realize that the more requirements that are added, the more questions/interpretations of words that can result from the requirement. Registered entities become more subject to violations not because they have neglected to protect their BES Cyber Systems, but rather because of differences in understanding of the words of a requirement - all the while the intent of the requirement had never really been “violated”.
26.27	FirstEnergy Corporation	Disagree	Need clarification wireless technology (does it include Wi-Fi, Bluetooth, Routable Protocol).

#	Organization	Yes or No	Question 26 Comment
26.28	National Grid	Disagree	o National Grid recommends changing 11.1 to “Identify the use and security restrictions for wireless technologies”. Are smart phones which have wireless capabilities considered as wireless technologies? Suggest providing examples of wireless technologies in the guidance document. o For 11.2 and 11.3 National Grid recommends changing from “Required for external connectivity only” to “Required” since the criteria already limits the scope to “remote access”
26.29	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.30	Puget Sound Energy	Disagree	Puget Sound Energy requests clarity to NERC’s definition of “wireless”. If NERC means the 802.1x protocol, then it should specify that so as not to confuse entities with radio telecommunication networks and other wireless technologies.
26.31	LCEC	Disagree	R11 - Any wireless portion of a control or administrative session should be included. Remove the term remote and replace with non-console.Many issues surrounding wireless including encryption and open transport, relay communication, PLCs. Need to clearly define scope and expectations.
26.32	ISO New England Inc	Disagree	R11.1 - Is this just a policy statement and belong in R1 or does it need to be enforced and detect violations of the restrictions? How can this be audited? If there are no restrictions is this a violation?For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”
26.33	Ameren	Disagree	R11.1 what is meant by "use Restrictions" does this apply to the type of device allowed to be used on wireless, of the type of use allowed on wireless technology. Please add more detail on this requirement.R11.2 and R11.3 - Does this include Serial communications such as RTU connectivity or other non-routable protocols? Please

#	Organization	Yes or No	Question 26 Comment
			add more description in these requirements.
26.34	Northeast Power Coordinating Council	Disagree	Recommend changing 11.1 to “Identify the use and security restrictions for wireless technologies”.For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
26.35	Detroit Edison	Disagree	Remove requirement 11.1. Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.R11, R12 and R14 use term “remote electronic access” and R13 uses the term “remote access”. Revise to maintain consistency.
26.36	WECC	Disagree	Requirements R11 and R12 could be combined into a requirement to produce and implement a Remote Access Plan.There are no specific requirements regarding use restrictions on wireless technologies. This criterion cannot be audited.”Wireless” and “remote electronic access” are two different things and should be addressed in separate requirements.There are no specific requirements regarding remote access. These criteria cannot be audited.
26.37	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that the definition be reworded to say "...a device external to the BES Cyber System's network.”
26.38	Network & Security Technologies Inc	Disagree	Section is unclear. Is wireless an example of a technology that might be employed for remote access, or is the SDT positing other uses? Please clarify. In addition, beyond 11.3, section does not contain any explicit requirements for controlling remote access. 11.1 and, possibly, 11.2 as written would more appropriately be included in a policy (R1). Requirements in R11 should be more aimed towards enforcement of “use restrictions” and exclusion of access methods that are not explicitly allowed.

#	Organization	Yes or No	Question 26 Comment
26.39	American Electric Power	Disagree	Security controls for wireless access seem out of place in the remote access area. Wireless Access controls is a form of boundary protection for the network and should be moved to R20-R22.
26.40	Manitoba Hydro	Disagree	Since Requirement R11 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns and should be removed. Requirement 11.3 is unclear if it refers to authorizing remote access as a design, or operational requirement, or does it refer to the authorization of user access and privileges? Please clarify.
26.41	Entergy	Disagree	Suggest breaking out wireless access from other remote access. These are two distinct technology types, and breaking out within this document the use restrictions and minimum security countermeasures (e.g., WPA, WPA2) for wireless technologies is appropriate.
26.42	Alberta Electric System Operator	Disagree	The AESO believes that wireless access and remote access should be two separate concepts.
26.43	E.ON U.S.	Disagree	The definition of remote access includes the criteria “...from a device external to the BES Cyber System . . . “ With the removal of the concepts of an electronic security perimeter, the boundaries to these systems are not clearly defined, and “external” becomes difficult to determine. It is unclear, for example, whether accessing a BES Cyber System from an internal workstation (though external to the BES Cyber System) constitutes remote access. The definitions for BES Cyber System and BES Cyber Component also do not address the concept of a perimeter.
26.44	Kansas City Power & Light	Disagree	The scope of “wireless” is not clear and can result in interpretation issues throughout these requirements.
26.45	Consultant	Disagree	There is no difference in "remote access" and "wireless electronic access" as remote access is defined in the standard. Suggest deleting reference to wireless electronic

#	Organization	Yes or No	Question 26 Comment
			access in requirement. But if you must have wireless addressed, include it in the definition of remote access.R11. This phrasing is awkward - "to ensure that no unauthorized access is allowed to its BES Cyber Systems" Suggest using wording comparable to R8 "to maintain control of access to its BES Cyber Systems." Table R11 - 11.1 Removing the wireless term from the requirement eliminates the need for this item. Suggest deleting this item.Item 11.3 - This is an account management requirement, and should be moved to R8, and deleted from R11.Item 11.2 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"
26.46	Northeast Utilities	Disagree	There is not enough information provided - please specify minimum acceptable security standard allowed (i.e., two-factor, level of encryption, etc.) associated with the use of wireless technologies.
26.47	Emerson Process Management	Disagree	This is a very confusing requirement. Remote does not equal to wireless.The requirement states "allows remote OR wireless electronic access.." The table title is "Wireless AND Remote..."If a remote access is carried out through wired VPN, doesn't this table apply?Does this "remote access" only emphasize on "interactive user session?" If so, this requirement is not applicable to wireless I/O when only data are transmitted to and from BES Cyber System via wireless communications.
26.48	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
26.49	Hydro One	Disagree	We don't understand why the wireless communication is getting special attention. We believe that the protection should remain the same regardless of the type of access point (i.e if it is wired, Wi-Fi, ZigBee etc.). Please explain the rational behind the decision.Recommend changing 11.1 to "Identify the use and security restrictions for wireless technologies".For 11.2 and 11.3 recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope to

#	Organization	Yes or No	Question 26 Comment
			"remote access".
26.50	We Energies	Disagree	We Energies agrees with EEI: Given the local definition of Remote access, the requirements of Table 11 Row 11.2 are extremely unclear.We Energies agrees with EEI: The requirements of requirements of Table 11 Row 11.3 appear to be duplicative of R8.1 and should be removed.
26.51	RRI Energy	Disagree	While the statement 'an interactive user session with a BES Cyber System" is clear to me, examples of "interactive non-user" should be clarified so that the users of this standard know when R11 does not apply. The most common non-user interaction, I would term as "interactive application session". One prevalent wireless "interactive application session" would be a GPS antenna to time synch a cyber asset. Another example would be a wireless serial data IO application. Since these are non-user sessions, R11 does not apply.
26.52	US Army Corps of Engineers, Omaha Distirc	Disagree	Wireless and remote access should be separated.
26.53	NextEra Energy Corporate Compliance	Disagree	Wireless and remote electronic access should be two distinct and separate categories of requirements. Wireless should be defined and it should be established that the term wireless in the context of the requirements is a technology based on 802.1X. As it stands right now, wireless could additionally be considered both blue tooth and radio technologies.Moreover, interactive user session needs to be defined and clarified. It should explain if interactive includes a user session where the user only has read capabilities or if an interactive user session is only applicable when the end user had modification capabilities to the BES Cyber System component. It is unclear how requirement 11.1 adds to the reliability or security of the BES Cyber system. Are the use restrictions per user or are these network restrictions? Moreover, if a Responsible Entity's documented use restrictions are overly broad and insecure, they still comply with the requirement as is. The recommended approach should provide guidelines on acceptable means of securing wireless access to BES Cyber System

#	Organization	Yes or No	Question 26 Comment
			components.Requirement 11.2 should be modified to include the requirement for strong technical and procedural controls for remote access. Requirement 11.3 is vague and unclear as it is currently stated. A responsible entity could misinterpret the requirement for establishing and implementing a defined process for authorizing the establishment of remote access and associated remote access privileges to approve the initial remote access infrastructure and not approving each individual that has remote access capabilities.Requirement 11.3 should be worded to state the following, “If remote access is used and/or implemented, establish, and implement a defined process for authorizing the establishment of remote access infrastructure”NextEra suggests an additional requirement be added and stated as follows:”If remote access is used and/or implemented, establish a defined process for authorizing users to utilize remote access for unescorted interactive cyber access to BES Cyber Systems.”There are not any requirements related to logging or monitoring of remote electronic access and the current requirements within Boundary Protection (R20-R22) requirements do not address this issue either.Finally in 11.2 and 11.3, why make the distinction for "for external connectivity only" rather than just stating that it is "required"? When remote access is used and/or implemented, does it imply "external" connectivity based on the local definition?
26.54	Platte River Power Authority	Disagree	Wireless technology shouldn’t be specifically called out in the standards. Security controls should be broad enough to cover all technologies including wireless and should be handled in their respective sections.

27. Do you agree with the definition of remote access as proposed for this standard? Please explain and provide any suggestions for modification.

Summary Consideration:

The remote access requirements from CIP-011-1 have been moved to CIP-005-5 - Cyber Security - Electronic Security Perimeters – Requirement R2.

Commenters expressed concern that the Standards need better definitions to clarify remote access vs. external access. In response, a new requirement for Remote Access Management (CIP-005-5 R2) for Interactive Remote Access was created based on the Urgent Action Revisions to CIP-005-3.

Commenters expressed that there should be some governance of automated data exchange with remote systems. In response, the SDT noted that automated data exchange (or data in motion) requirements are not considered within scope of this Standard.

The SDT has proposed three formal definitions to provide greater clarity around external connectivity and remote access as they apply to NERC's Reliability Standards:

External Connectivity: *Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.*

External Routable Connectivity: *The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.*

Interactive Remote Access: Any user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

#	Organization	Yes or No	Question 27 Comment
27.1	WECC		Consider renaming to Remote User Access since it is specific to user not other systems or machines. Move to the beginning of the standard. Don't like box in the middle of requirement.Additional language should be added to clarify what constitutes a remote interactive session.

#	Organization	Yes or No	Question 27 Comment
27.2	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	Definition is good, but please see comments for questions 1.a and 1.b.
27.3	Exelon Corporation	Agree	Exelon would like clarity on whether “view only” access would be included in the definition of “interactive user session”? If the answer is no, this should be explicitly stated in the definition of remote access.
27.4	Dairyland Power Cooperative	Agree	However, there should be some governance of automated data exchange with remote systems, perhaps in another section. Also, there is no governance as to how wireless technology can be used for non-interactive data communications.
27.5	Alliant Energy	Agree	However, we recommend consideration of adding clarity to the use of the term “external” in the definition or the replacement of the word “external” with “geographically or logically separate”.
27.6	Consultant	Agree	If "wireless access" has to be specifically stated it should be included in the definition as a method of remote access.
27.7	Southern California Edison Company	Agree	Remote Access is defined without reference to boundaries, logical or physical. For example, access from any device residing in the same local area network, but not part of the BES Cyber System, can be interpreted as Remote Access.
27.8	Florida Municipal Power Agency	Agree	The review periods of the access may need to change with the different levels (12 months for low, 6 for medium, and 4 for high). The standard should require end-to-end encryption between the BES Access Point and the endpoint. Wireless should require minimum standards for 802.11 access points, such as WPA/AES encryption.
27.9	Progress Energy (non-Nuclear)	Agree	This can imply a non routable protocol since a command to open a breaker does result in an operation and provides a subsequent indication that the breaker actually

#	Organization	Yes or No	Question 27 Comment
			did open.
27.10	FirstEnergy Corporation	Agree	We agree fundamentally with the definition, but are concerned about impact to areas outside the BES Cyber System (e.g. Remote access to corporate networks bordering the BES Cyber Systems). Need clarity of "interactive user session".
27.11	Xcel Energy	Agree	We feel it would be beneficial to define the remote access point. For example, a case where a user uses a desktop VPN access to dial-up access a substation relay.
27.12	Independent Electricity System Operator	Disagree	- For 11.2 and R11.3 is Required for external connectivity only. If you connect remotely, how is this not external connectivity to the BES Cyber system - shouldn't these entries just be "required"
27.13	PacifiCorp	Disagree	(See comments on #13) The problem is conflicting definitions. The BES Cyber System Component definition requires that any device providing "control" of the BES Cyber System is to be considered a component of the BES Cyber System. (pg 2, Standard CIP-010-1) Yet, remote access is defined as an "interactive user session with a BES Cyber System from a device external to the BES Cyber System". (pg 12, Standard CIP-011-1)In short, all devices providing 'control' must be considered "BES Cyber System Components", which corresponds to 'internal access'. This definition eliminates remote access that provides control, because the provided function of 'control' requires reclassification as 'internal'.
27.14	US Army Corps of Engineers, Omaha Distirc	Disagree	Agree with general concept of remote access referring to an interactive session from an external location. Definition of external to BES Cyber System is poorly defined. Requirement is too stringent. Breaking systems up into small groups to provide levels of control and protection appropriate to the group of components would be common good practice. This requirement would seem to restrict communication among BES Cyber Systems within a facility and make them cumbersome to manage and protect at appropriate levels. entities need more leeway in defining communication amongst systems and different levels would apply between different systems.

#	Organization	Yes or No	Question 27 Comment
27.15	MRO's NERC Standards Review Subcommittee	Disagree	As written, the definition could be interpreted to include simple data exchanges between an RTU and a SCADA master, although we do not believe this was the intent of the drafting team. We would propose adding the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
27.17	The Empire District Electric Company	Disagree	Comments: As written, the definition could be interpreted to include simple data exchanges between an RTU and a SCADA master, although we do not believe this was the intent of the drafting team. We would propose adding the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.18	Luminant	Disagree	Controls for Remote access should include only the machines that have direct acces.
27.19	Network & Security Technologies Inc	Disagree	Current definition suffers from inadequacy of the definition of "external connectivity." As suggested in our response to Question 13, we think the definition might be helped by recasting it as meaning interactive access to a BES Cyber System from "outside" an electronic boundary such as an ESP.
27.20	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy is concerned this definition would apply to laptop computers used to perform maintenance on programmable electronic devices and believes that a temporary laptop connection to perform maintenance on an on-site programmable electronic device does not involve the same process as a typical interactive user session through remote access. Therefore CenterPoint Energy believes this requirement should not apply to temporary laptop connections which are otherwise in compliance with section R26 and recommends an exception be included.

#	Organization	Yes or No	Question 27 Comment
27.21	E.ON U.S.	Disagree	E.ON U.S. suggests that the standard specify access is through an “access point”.
27.22	RRI Energy	Disagree	Give more clarity on non-user sessions so that it is well understood that application data sessions are not a part of the “remote access” terminology of R11.
27.23	San Diego Gas and Electric Co.	Disagree	If a device can establish an interactive user session with a BES Cyber System and thus either respond to a BES condition or disturbance or enable control and operation, this “external device” should be named a “BES Cyber System Component.SDG&E recommends that the definition be reworded to say "...a device external to the BES Cyber System's network.”
27.24	US Bureau of Reclamation	Disagree	In addition, however, a mechanism needs to needs to be established to deal with devices locally connected for the purpose of "testing" and "configuration" so that these devices can be periodically connected for a specified and limited purposes. Per discussions during the recent Grapevine, TX, meeting, the drafting teams indicated that they would address this issue during their revision process.
27.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
27.26	National Grid	Disagree	National Grid recommends this definition be consistent with the “external connectivity” definition -recommend changing from “from a device external to the BES Cyber System” to “from a device external to the BES Cyber System Boundary”.
27.27	Black Hills Corporation	Disagree	Need a better definition to clarify remote access vs. external access. This creates policy issues for entities with respect to their definitions of these terms.
27.28	Northeast Utilities	Disagree	Need to clarify external connectivity (i.e., from other security domains within the company’s internal network or directly from the public internet). Level of authentication required should differ.

#	Organization	Yes or No	Question 27 Comment
27.29	LADWP	Disagree	Needs more clarification
27.30	NextEra Energy Corporate Compliance	Disagree	NextEra suggests defining external connectivity should be defined and clarified. It is unclear if external connectivity means external to the network the BES Cyber System resides or if it means connectivity from any device to any BES Cyber System component whether it is on the same network. External connectivity should be defined as any remote connection established through the BES Cyber System network access point devices, which includes examples of access point devices, such as dial-up connections, firewalls, SSL VPN connections, etc to a BES Cyber System component. As a point of clarification, since remote access is defined as "an interactive user session with a BES Cyber System from a device external to the BES Cyber System", is the device external to the BES Cyber System now considered a BES Cyber System with the same BES Impact Level as the BES Cyber System in which the device is remotely connecting to? For example, if we have a High Impact BES Cyber System which is an Energy Management System (EMS) within a Control Center, a laptop is used to remotely connect to this EMS, is the laptop now considered a High Impact BES Cyber System?
27.31	Tenaska	Disagree	not needed
27.32	USACE - Omaha Anchor	Disagree	Per your definition one cyber system talking to another cyber system that are side by side would be considered remote access - there seems to be no way to mitigate this. Remote access would be better served defined as communication from outside of the “physical security perimeter” or outside the plant.
27.33	Con Edison of New York	Disagree	R11 dialog box refers to Remote access as an interactive session with a BES Cyber System from a device “external” to a BES Cyber System. It is expected that external means from outside the electronic boundary.
27.34	Hydro One	Disagree	Recommend this definition be consistent with the “external connectivity” definition - recommend changing from “from a device external to the BES Cyber System” to “from

#	Organization	Yes or No	Question 27 Comment
			a device external to the BES Cyber System Boundary".
27.35	ISO New England Inc	Disagree	Recommend this definition be consistent with the "external connectivity" definition - recommend changing from <<from a device external to the BES Cyber System >> to << from a device external to the BES Cyber System Boundary>>
27.36	Northeast Power Coordinating Council	Disagree	Recommend this definition be consistent with the "external connectivity" definition - recommend changing from "from a device external to the BES Cyber System" to "from a device external to the BES Cyber System Boundary".
27.37	American Electric Power	Disagree	Regarding "Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the BES Cyber System", should this be "Remote electronic access"? Table R11 refers to "Wireless and Remote Electronic Access Documentation". Adding "electronic" to the definition would maintain consistency.
27.38	Regulatory Compliance	Disagree	Remote access - access originating from outside the eletronic boundary.
27.39	Southwest Power Pool Regional Entity	Disagree	Remote access can be application-to-application and should not be limited to just interactive access. For example, an FTP file transfer works the same way whether invoked interactively by a human user or programmatically by an application. It makes no sense to establish requirements for interactive access only.
27.40	Duke Energy	Disagree	See above, external to station. For generation stations in particular, external connectivity (R3) and remote connectivity (R11, R12, R13) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Same for R13.The definition may need to state "a device external to the BES Cyber System and outside the BES Cyber System electronic boundary".

#	Organization	Yes or No	Question 27 Comment
27.41	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary.
27.42	Allegheny Energy Supply	Disagree	Suggest clarifying similar to the following: Remote access should be interactive access of a BES Cyber System from a device external to the electronic and physical protection boundaries of that BES Cyber system.
27.43	Platte River Power Authority	Disagree	Suggested Revision:Remote access for the purpose of this standard means an interactive user session with a BES Cyber System Component from a device external to the BES Cyber System.That would better match the definition of external connectivity.
27.44	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS proposal to add the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".
27.45	Minnesota Power	Disagree	The current definition of "remote access," along with definition of "external connectivity," leaves open to interpretation whether Requirement R11 applies to host-based controls, or if it mandates network-based controls even within isolated or protected networks. It would appear that any interactive network access to a BES Cyber System is by definition remote access unless a portion of the network is included in the definition of that particular BES Cyber System. If the latter approach is adopted then multiple, otherwise independent, BES Cyber Systems might be arbitrarily selected to be a single BES Cyber System in order for this requirement to be met and still allow for reasonable security management.
27.46	Detroit Edison	Disagree	The definition may be interpreted to include maintenance devices. Revise as follows "Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the Electronic Boundary of the BES Cyber System."

#	Organization	Yes or No	Question 27 Comment
27.47	Ameren	Disagree	The phrase "from a device external to the BES Cyber System," is open to interpret. Please clarify if this refers to a device physically external or electrically external.â€,â€,â€,
27.48	Alberta Electric System Operator	Disagree	The word “user” should be removed from “interactive user session” because it implies human interaction and does not consider automated malware.
27.49	Progress Energy - Nuclear Generation	Disagree	This definition is not clear to me. I recommend Remote Access be defined based on NIST 800-53 Appendix B slightly modified to accommodate industrial control systems. “Access to a BES Cyber Security System by a user or process communicating from an untrusted network”
27.50	Bonneville Power Administration	Disagree	This has the same issues as the definition of "External Connectivity". In fact, the definition could simply be "an externally connected interactive user session. Recommend that the definition be reworded to use the definition of External Connectivity, along with a suitable redefinition of that term, as described in question 13. If not, recommend - "Remote Access - For the purposes of this standard, remote access is defined as an electronic connection with control capabilities to a BES Cyber System, using a data communications path that encompasses, in some or all portions, links outside the control of the Responsible Entity. "Also add a definition of wireless access that makes it clear that such access is always an example of external connectivity. The definition should exclude such protocols as Bluetooth and infrared, which are intra-system, not inter-system methods. Note that even non-interactive wireless access should be controlled.Suggestion: Wireless electronic access for the purpose of this standard means access to or from a BES Cyber System to another cyber system using wireless communications. Even if both systems and any wireless access points are under the control of the Responsible Entity, the wireless communications path itself is not. For that reason, any wireless electronic access is considered to be external connectivity."

#	Organization	Yes or No	Question 27 Comment
27.51	Kansas City Power & Light	Disagree	This is too broad and could include devices such as Remote Terminal Units.

28. Table R11 provides direction concerning what impact level of BES Cyber Systems to which Requirement R11 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R11 has moved to CIP-005-5- Cyber Security - Electronic Security Perimeters, Requirement R2.

Commenters expressed concern that for items R11.2 and R11.3, given the definitions provided in the standard, how is remote access provided without external connectivity? The SDT agrees and notes that a new requirement for Remote Access was created based on the Urgent Action Revisions to CIP-005-3.

Commenters also expressed concern that there are inconsistent definitions for "external connectivity" and "remote access". The SDT has proposed three formal definitions to provide greater clarity around external connectivity and remote access as they apply to NERC's Reliability Standards:

External Connectivity: Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.

External Routable Connectivity: The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.

Interactive Remote Access: **A**ny user interactive access by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

#	Organization	Yes or No	Question 28 Comment
28.1	WECC		Again consider replacing with requirement for remote access plan that provides specific requirements and conditions for remote access.
28.2	Florida Municipal Power Agency	Agree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the

#	Organization	Yes or No	Question 28 Comment
			BES Cyber System.
28.3	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
28.4	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
28.5	Bonneville Power Administration	Agree	This agreement assumes that External Connectivity is suitably redefined. Also, consider the following changes:1 - Remove Wireless from the title and the requirements.2 . If wireless is to be addressed, add a new requirement item specifically for wireless, dealing with the requirements on wireless access that are in addition to those for remote access in general.
28.6	E.ON U.S.	Disagree	: E.ON U.S. does not believe that compliance requirements are necessary for low impact systems
28.7	Southwest Power Pool Regional Entity	Disagree	“Required for external connectivity only” does not make sense. A properly configured wireless access should never directly connect within the secured network, thus any access will be “external.”
28.8	Luminant	Disagree	11.2 and 11.3 should be for Routable External Connectivity only
28.9	American Electric Power	Disagree	11.2: Regarding "If remote access is used and/or implemented, document the allowed methods for remote access", does this mean the list of approved ports and services? If not, what is meant by "allowed methods"?
28.10	US Army Corps of Engineers, Omaha Distirc	Disagree	Agree with general concept of remote access referring to an interactive session from an external location. Definition of external to BES Cyber System is poorly defined.

#	Organization	Yes or No	Question 28 Comment
			Requirement is too stringent. Breaking systems up into small groups to provide levels of control and protection appropriate to the group of components would be common good practice. This requirement would seem to restrict communication among BES Cyber Systems within a facility and make them cumbersome to manage and protect at appropriate levels. entities need more leeway in defining communication amongst systems and different levels would apply between different systems.
28.11	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protction and type of access granted.
28.12	Black Hills Corporation	Disagree	Applicability needs to be consistent previous non-wireless requirements.
28.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
28.14	LCEC	Disagree	Clarify what is meant by external connectivity only. Is this referring to any access to a BES cyber system component as defined earlier in the standard?
28.15	The Empire District Electric Company	Disagree	Comments: For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.16	Platte River Power Authority	Disagree	Disagree with the inclusion of Wireless.
28.17	Hydro One	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
28.18	ISO New England Inc	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”

#	Organization	Yes or No	Question 28 Comment
28.19	Northeast Power Coordinating Council	Disagree	For 11.2 and 11.3 recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
28.20	American Transmission Company	Disagree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.21	MRO's NERC Standards Review Subcommittee	Disagree	For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
28.22	NextEra Energy Corporate Compliance	Disagree	For Low Impact BES Cyber Systems, (1) documenting the allowed methods for remote access per 11.2, and (2) establishing and implementing a defined process for authorizing the establishment of remote access and associated remote access privileges per 11.3 should not be required. The identification of use restrictions for wireless technologies per 11.1 should be a sufficient security management control for Low Impact BES Cyber Systems. 11.2 and 11.3 will be administratively burdensome if required for practically every BES Cyber System.
28.23	San Diego Gas and Electric Co.	Disagree	Instead of defining requirements by using the impact levels, SDG&E feels it would be more appropriate to factor in the level of risk associated with the BES Cyber Systems to define the requirements for wireless and remote access.
28.24	Dairyland Power Cooperative	Disagree	Is external connectivity considered to be from outside the entity’s premises, or is it considered to be from outside the protected BES system (including for instance a corporate LAN). If it means outside the premises, then it seems deficient to not document the access-especially when later enabling of external connectivity could occur without the involvement of the supporting the BES cyber system. If it means external to the BES cyber system, then “external connectivity” and “remote access”

#	Organization	Yes or No	Question 28 Comment
			are redundantly used in 11.2 and 11.3.
28.25	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
28.26	FirstEnergy Corporation	Disagree	Need clarification on "external connectivity", because the nature of remote is external.
28.27	National Grid	Disagree	o For 11.2 and 11.3 National Grid recommends changing from “Required for external connectivity only” to “Required” since the criteria already limits the scope to “remote access” o National Grid also suggests deleting the requirement 11.3 for Low Impact BES CS.
28.28	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’. Without understanding the defined intent suggested specific changes may be vague. Remote access is defined but not external connectivity. Is there a distinction?
28.29	American Municipal Power	Disagree	Please provide a little or no impact category
28.30	BGE	Disagree	Remove the requirement for Low on 11.1, 11.2 and 11.3
28.31	Garland Power and Light	Disagree	Requirement 11.1, 11.2, 11.3 - remove Low Impact classification from all 3
28.32	Detroit Edison	Disagree	Requirements 11.2 and 11.3 specify “Required for external connectivity only”. This is redundant. It is not possible to have remote access without external connectivity by definition.
28.33	Emerson Process Management	Disagree	Since this standard is for remote access, is the "external connectivity" potentially redundant or extra? If there is no external connectivity, how can user establish an interactive session remotely?

#	Organization	Yes or No	Question 28 Comment
28.34	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary.
28.35	ERCOT ISO	Disagree	Table 11 should address remote and wireless access across all requirements in keeping with the title of the section.
28.36	Consultant	Disagree	Table R11 - 11.1 Removing the wireless term from the requirement eliminates the need for this item. Suggest deleting this item.Item 11.3 - This is an account management requirement, and should be moved to R8, and deleted from R11.Item 11.2 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"There is an inconsistency between Table R11 and Table R12. If R11 requires all impact levels to have documented controls, then R12 should require account management controls for all impact levels. To be consistent with previous account management requirements, the account management controls should be applied to medium & high impact systems, and removed from low impact systems, and Table R11 items should not be required for low impact systems. Or all impact levels should be required in both R11 & R12.
28.37	Alberta Electric System Operator	Disagree	The AESO suggests moving row 11.1 in Table R11 to a separate section governing wireless as a standalone requirement.
28.38	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS comment that “for external connectivity only” is redundant and should be removed from R11 Table 11.2 and Table 11.3 impact levels.
28.39	Reliability & Compliance Group	Disagree	the external connectivity qualifier
28.40	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create

#	Organization	Yes or No	Question 28 Comment
			confusion regarding the applicability of the criteria for each impact level.
28.41	US Bureau of Reclamation	Disagree	The level for Low Impact is not consistent with Electronic Access Management requirement in R8.

29. Requirement R12 of draft CIP-011-1 states "Each Responsible Entity that allows wireless and remote electronic access to any of its BES Cyber Systems shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management to ensure that no unauthorized access is allowed to its BES Cyber System." Do you agree with the list of criteria that is included in Requirements Table R12? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each item as represented in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R12 has moved to CIP-005-5 – Cyber Security - Electronic Security Perimeters, Requirement R2

Commenters suggested the need to separate wireless and remote access, and Requirement R12.1 appears to be duplicative of R8.2 and has been removed. The SDT agrees and notes a new requirement for Remote Access was created based on the Urgent Action Revisions to CIP-005-3, and the wireless access requirements have been removed.

Several commenters suggested that R8 and R12 are duplicative as both require quarterly review and verification of accounts and associated access privileges. The SDT moved all requirements for verification of accounts and associated access privileges into the revised CIP-004-5.

Other commenters suggested this requirement should have increased applicability (Low, Medium, and High rather than High only). In response, the SDT notes that the applicability for remote access requirements extends to Medium Impact BES Cyber Systems. The SDT does not feel it necessary to extend this requirement to Low Impact BES Cyber Systems. The SDT does not feel that the risk reduction for reliability justifies the administrative overhead of applying this requirement to all Low Impact BES Cyber System.

#	Organization	Yes or No	Question 29 Comment
29.1	WECC		See comments for R10/R11 consider combining this into a requirement for a Wireless Plan and Remote Access PlanThis requirement could be rolled into R8.
29.2	Southern California Edison Company	Agree	Additional clarification may be provided on criteria for control systems. It seems that a control center is temporally viewed as a distributed control system; each node (footprint restricted to one facility but electronically extends scope of control to at least one other facility) can be treated as a "control center". The drafting team should

#	Organization	Yes or No	Question 29 Comment
			develop a guideline document that presents a discussion of the local definition of a control center as a facility or system that has the ability to control more than one BES asset, side by side, with definition of the electronic boundaries of a BES system. Remote access within a facility and from beyond a particular physical facility can have different risk profiles.
29.3	Southwest Power Pool Regional Entity	Agree	Agree with the wording as presented. See comments to question 30 about applicability.
29.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
29.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Consider combining R7, R8, R11 and R12.
29.6	MRO's NERC Standards Review Subcommittee	Agree	Note impact level comments under question 30.
29.7	Progress Energy - Nuclear Generation	Agree	R12 can be improved by incorporating information contained in attached Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
29.8	BCTC	Agree	Suggest rewording from Wireless and Remote Electronic Access to Wireless or Remote Electronic Access
29.9	Bonneville Power Administration	Agree	The objective of this requirement ("to ensure that no unauthorized access is allowed to its BES Cyber System") should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that

#	Organization	Yes or No	Question 29 Comment
			the Responsible Entity must take.Our agreement with this Requirement is contingent on the redefinition as discussed in Question 27 and the definition of wireless electronic access stated above.
29.10	GTC & GSOC	Agree	We generally agree but disagree with the inclusion of the term Wireless in the requirement and associated table. Neither have anything to do with wireless as distinguished from other remote access.
29.11	Independent Electricity System Operator	Disagree	- R12 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.
29.12	Luminant	Disagree	12.1 should be for Routable External Connectivity only
29.13	US Bureau of Reclamation	Disagree	Access management should be established for all impact lelvels. If the requirements of R11 are going to be established, R12 needs to be established to support enforcement. Further, what is meant by quarterly review.
29.14	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
29.15	Black Hills Corporation	Disagree	Do not understand why wireless has its own table. Even if the overall requirement is a little more difficult, consistency of approach will result in greater security.
29.16	Entergy	Disagree	Entergy agrees with the list of criteria, but believes it should apply equally to high, medium and low assets.We also suggest eliminating R12 and combine it with R8.2 (quarterly review and verification of accounts and associated access privileges), as these are part and parcel of account rights management.
29.17	Hydro One	Disagree	For consistency with 12.1, recommend removing “wireless” from R12.Recommend changing Requirement 12.1 from “quarterly review” to “annual review”. There are no additional benefits to the shorter review period.Similarly to our previous comment

#	Organization	Yes or No	Question 29 Comment
			to R11, we don't understand why the wireless communication is getting special attention. We believe that the protection should remain the same regardless of the type of access point (i.e. if it is wired, Wi-Fi, ZigBee etc.). Please explain the rational behind the decision.
29.18	ISO New England Inc	Disagree	For consistency with 12.1, recommend removing "wireless" from R12R12 combines Wireless and Remote access. It is suggested that this be broken out in to separate requirements. Seems like an assumption that if you are connecting via wireless you are remote - not always the case.
29.19	Northeast Power Coordinating Council	Disagree	For consistency with 12.1, recommend removing "wireless" from R12.Recommend changing Requirement 12.1 from "quarterly review" to "annual review". There are no additional benefits to the shorter review period.
29.20	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). As written, the requirement in R12 for remote access is particularly burdensome. Table 12 o redundant with Table 11 and Table 8. Suggest including this review as part of the review conducted in 8.2. o suggest removing 'and verification.' We don't understand the benefit to this and question if it is possible for remote access.
29.21	Constellation Power Source Generation	Disagree	In general, Constellation believes that wireless controls should be combined with network controls, as the same controls will be applied.
29.22	Southwestern Power Administration	Disagree	Is a separate requirement for wireless access really necessary when a requirement already exists for protecting access to a BES Cyber System by any means of entry? If so, then suggest separating wireless from remote access.

#	Organization	Yes or No	Question 29 Comment
29.23	Northeast Utilities	Disagree	It is our belief that the review of access privileges conducted under Requirement 8 would satisfy the intent of this requirement as well and that R12 should be eliminated.Hence, this requirement is not needed as long as it is clear that remote access will not be granted unless explicit specific rights are granted to some asset they connect with. Access should not be given access to a protected area unless there is a need to access a specific asset, i.e., there is no business need to just grant network only access.
29.24	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with SPP's observation below:We question the need for a specific requirement for wireless devices. We understand there have been inquiries about treatment of wireless devices. But a wireless access point has the same impact on a BES Cyber System as any other access point. A requirement to protect access to a Cyber System already includes any possible means of entry. The use of a wireless device to access a BES Cyber System can be determined with an audit of access logs and a further audit of control of that access would reveal whether appropriate protections were in place. There is not a need for a separate distinct requirement subject to records retention and audit for specific wireless devices. NERC must realize that the more requirements that are added, the more questions/interpretations of words that can result from the requirement. Registered entities become more subject to violations not because they have neglected to protect their BES Cyber Systems, but rather because of differences in understanding of the words of a requirement - all the while the intent of the requirement had never really been “violated”.
29.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes that if remote access is used and/or implemented, document and implement a quarterly review and verification of the personnel with remote access and their associated access privileges, it is unclear how this access is supposed to be verified and what is accepted as part of the verification process. This is the same as the comments to address question #20 of this questionnaire. If remote access is used and/or implemented, documenting and implementing a quarterly review and verification of the personnel with remote access and their associated access privileges

#	Organization	Yes or No	Question 29 Comment
			may not be sufficient. This process needs to be tied in with personnel (1) gaining authorized remote access to a BES Cyber System, (2) modifying their access privileges to a BES Cyber System due to change of the user's access rights due to change in role or responsibility and, (3) loosing authorized remote access to a BES Cyber System due to a revocation of electronic access to a BES Cyber System.
29.26	National Grid	Disagree	o National Grid recommends an annual review for verification since quarterly review does not have much benefit. o National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access”
29.27	Progress Energy (non-Nuclear)	Disagree	Quarterly seems to be too frequent - propose 6 months or longer. We are required in R9 to revoke access for those that are terminated or do not need access within 72 hours.
29.28	LCEC	Disagree	R12 - 12.1 is covered in the account review requirements in R8. This should be changed to review the need for wireless as opposed to wired connectivity and reviewed annually.
29.29	Consultant	Disagree	R12 is an account management requirement. The requirement should be moved to R8 as an aspect of account management.There is no difference in "remote access" and "wireless electronic access" as remote access is defined in the standard. Suggest deleting reference to wireless electronic access in requirement. But if you must have wireless addressed, include it in the definition of remote access.R12. This phrasing is awkward - "to ensure that no unauthorized access is allowed to its BES Cyber Systems" Suggest using wording comparable to R8 "to maintain control of access to its BES Cyber Systems."
29.30	CWLP Electric Transmission, Distribution and	Disagree	R12. Due to the requirements access revocation in R9 this requirement should be extended to an annual review.

#	Organization	Yes or No	Question 29 Comment
	Operations Department		
29.31	Southern Company	Disagree	R12.1 addresses remote access only and does not include wireless, the table title and R12 includes wireless.
29.32	Allegheny Energy Supply	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.33	Allegheny Power	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.34	EEI	Disagree	Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.35	PNM Resources, Inc.	Disagree	Requirements for disabling access or user accounts in periods that are less than 6 hours are unrealistic, especially on weekends or during off-hours.
29.36	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that the wireless and remote electronic access management apply to devices external to the BES Cyber System's network.
29.37	Manitoba Hydro	Disagree	Since Requirement R12 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns and should be removed. Consider adding a requirement for securing the wireless access point.
29.38	ERCOT ISO	Disagree	Table 12 should address remote and wireless access across all requirements. 12.1: Should be combined with other access management requirements (physical, cyber, information).
29.39	BGE	Disagree	Tables 11 and 12 are out of synch.
29.40	Kansas City Power & Light	Disagree	The scope of “wireless” is not clear and can result in interpretation issues throughout these requirements.
29.41	FirstEnergy Corporation	Disagree	The Table is titled “Wireless and Remote ...”For consistency we suggest that 12.1 be

#	Organization	Yes or No	Question 29 Comment
			revised to state "... personnel with wireless and remote access ..."
29.42	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
29.43	We Energies	Disagree	We Energies agrees with EEI: Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
29.44	Alberta Electric System Operator	Disagree	Wireless access and remote access should be two separate concepts.
29.45	Detroit Edison	Disagree	Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.R11, R12 and R14 use term "remote electronic access" and R13 uses the term "remote access". Revise to maintain consistency.Requirement 12.1 specifies "Required for external connectivity only". This is redundant. It is not possible to have remote access without external connectivity by definition.

30. Table R12 provides direction concerning what impact level of BES Cyber Systems to which Requirement R12 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R12 has moved to CIP-005-5 – Cyber Security - Electronic Security Perimiters, Requirement R2.

Commenters suggested a reword of this item to remove "for external connectivity only", since remote access cannot be granted without external connectivity. The SDT agrees and has made this change.

Other commenters suggested this requirement should have increased applicability (Low, Medium, and High rather than High only). In response, the SDT notes that the applicability for remote access requirements extends to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. The SDT does not feel it necessary to extend this requirement to Low Impact BES Cyber Systems. The SDT does not feel that the risk reduction for reliability justifies the administrative overhead of applying this requirement to all Low Impact BES Cyber System.

Several commenters suggested that R9 and R12 are duplicative. The SDT moved all requirements for revocation of access privileges into the revised CIP-004-5.

#	Organization	Yes or No	Question 30 Comment
30.1	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Consider combining R7, R8, R11 and R12. At minimum, R12 should be consistent with R8.
30.2	Kansas City Power & Light	Agree	In general, this appears appropriate, however, these tables require considerable thoughtfulness and to the extent these requirements may be altered for presentation in the formal comment period, final judgment is reserved.
30.3	Progress Energy (non-Nuclear)	Agree	See Comment 14.Not needed. There already is another requirement for cyber access reviews.
30.4	Northeast Utilities	Agree	Suggest eliminating R12 - see response to Question 29.

#	Organization	Yes or No	Question 30 Comment
30.5	Independent Electricity System Operator	Disagree	- For R12.1 is Required for external connectivity only. If you connect remotely, how is this not external connectivity to the BES Cyber system - shouldn't these entries just be "required"
30.6	ERCOT ISO	Disagree	12.1: Should apply to Medium Impact BES Cyber System.
30.7	Southern California Edison Company	Disagree	All forms of access documentation should be required along with the level of protection and type of access granted. Wireless technology needs full security and encryption in regards to any level of BES Cyber System.
30.8	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
30.9	USACE HQ	Disagree	At a minimum, 12.1 should be required for all impact levels. Requirement 11 creates a document of remote access procedure and who has the right to use it, but for low and medium impact systems it is not required to update the same as per requirement 12.1.
30.10	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
30.11	Tenaska	Disagree	Combine 12 and 13
30.12	The Empire District Electric Company	Disagree	Comments: For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.13	Alberta Electric System Operator	Disagree	Create additional requirements in Table R12 for Medium and Low impact levels. Suggest semi-annual review for Medium Impact, and Annual review for Low impact.
30.14	Black Hills Corporation	Disagree	Do not understand why wireless has its own table. Even if the overall requirement is

#	Organization	Yes or No	Question 30 Comment
			a little more difficult, consistency of approach will result in greater security.
30.15	Entergy	Disagree	Entergy agrees with the list of criteria, but believes it should apply equally to high, medium and low assets.
30.16	Duke Energy	Disagree	For generation stations in particular, external connectivity (R3) and remote connectivity (R11) should be defined as remote/external to the station rather than to the BES cyber system. There are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station).
30.17	American Transmission Company	Disagree	For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.18	MRO's NERC Standards Review Subcommittee	Disagree	For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.
30.19	Consultant	Disagree	Item 12.1 - The terminology "Required for external connectivity only" is redundant in this requirement. This requirement is about allowing external connectivity via remote access. Suggest deleting "for external connectivity only"There is an inconsistency between Table R11 and Table R12. If R11 requires all impact levels to have documented controls, then R12 should require account management controls for all impact levels. To be consistent with previous account management requirements, the account management controls should be applied to medium & high impact systems, and removed from low impact systems, and Table R11 items should not be required for low impact systems. Or all impact levels should be required in both R11 & R12.

#	Organization	Yes or No	Question 30 Comment
30.20	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
30.21	WECC	Disagree	Medium Impact should still have the requirement as well.This should apply to all impact levels.
30.22	National Grid	Disagree	National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access”.
30.23	FirstEnergy Corporation	Disagree	Need clarification on "external connectivity", because the nature of remote is external.
30.24	NextEra Energy Corporate Compliance	Disagree	NextEra believes that regarding 12.1, why make the distinction for "for external connectivity only" rather than just stating that it is "required"? When remote access is used and/or implemented, does it imply "external" connectivity based on the local definition?
30.25	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’.
30.26	American Municipal Power	Disagree	Please provide a little or no impact category
30.27	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Specifically, if 11.2 and 11.3 require documenting allowed methods and processes for remote access, then table 12 should require quarterly review of the access granted via 11.2 and 11.3. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.

#	Organization	Yes or No	Question 30 Comment
30.28	LCEC	Disagree	R12 - 12.1 is covered in the account review requirements in R8. This should be changed to review the need for wireless as opposed to wired connectivity and reviewed annually.
30.29	Hydro One	Disagree	Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend that Medium Impact BES Cyber System should be Required.
30.30	Northeast Power Coordinating Council	Disagree	Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend that Medium Impact BES Cyber System should be Required.
30.31	Southwest Power Pool Regional Entity	Disagree	Remote access should be periodically reviewed for all impact categories. Ideally, a more frequent review should be required for High impact systems.
30.32	Allegheny Energy Supply	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.33	Allegheny Power	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.34	EEI	Disagree	Requirement R12 appears to be duplicative of R8.2 and should be removed.
30.35	ISO New England Inc	Disagree	Should be across the board, and annually for allRecommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”
30.36	MidAmerican Energy Company	Disagree	Specific requirements for wireless devices are not necessary. Furthermore, requirement R12.1 is duplicative of R8.2.
30.37	ReliabilityFirst Staff	Disagree	Suggest “Required for external connectivity only” for Medium Impact in row 12.1.
30.38	Network & Security	Disagree	Suggest including Medium Impact systems with external connectivity.

#	Organization	Yes or No	Question 30 Comment
	Technologies Inc		
30.39	US Bureau of Reclamation	Disagree	Table R12 should be applied to all Impact levels in keeping with requirements established in R11.
30.40	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS that “for external connectivity only” is redundant and should be removed from R12 Table 12.1. The table should therefore read:R12 Table 12.1: Low Impact: N/AMedium Impact: N/AHigh Impact: Required
30.41	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create confusion regarding the applicability of the criteria for each impact level.
30.42	PacifiCorp	Disagree	The term verification needs further definition. Requirement R12.1 appears to be duplicative of R8.2 and should be removed.
30.43	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
30.44	We Energies	Disagree	We Energies agrees with EEI: Requirement R12 appears to be duplicative of R8.2 and should be removed.

31. Requirement R13 of draft CIP-011-1 states "Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 – Remote Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R13? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R13 has moved to CIP-004-5 – Cyber Security - Personnel and Training, Requirement R7.

Commenters suggested making the timeframes for revocation in R13 the same as R9. In response, the timeframes for revocation requirements have been simplified as follows:

- Revocation of access to BES Cyber Systems at the time of the termination or resignation and by by the end of the next calendar day for reassignments or transfers action,
- Revocation of access to BES Cyber System Information by by the end of the next calendar day for terminations or reassignments, and
- Additional requirements were added to address revocation of user accounts on BES Cyber Systems and shared accounts.

Commenters expressed concerns that persons who transfer are not automatically considered a threat to the system, and the timeframes for revocation should reflect this. In response, the requirement for transfers now states a review of access is required on the transfer date, and any unneeded access is revoked when it is no longer needed.

Commenters suggested keeping the revocation timeframes the same as defined in CIP Version 3. The SDT notes that FERC Order 706 directs revocation of access to occur immediately in all cases where access is no longer needed. The requirement has been modified to simply revoke access when a person no longer needs it. Organizations usually have termination procedures to return company property and perform exit interviews. Processes for revoking access (both physical and remote electronic) can be incorporated into an organization's termination and transfer procedures.

#	Organization	Yes or No	Question 31 Comment
31.1	WECC	Agree	Agree with criteria but recommend combining with R9 Revoking Access.This could be rolled into R9

#	Organization	Yes or No	Question 31 Comment
31.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
31.3	Florida Municipal Power Agency	Agree	Consider combining R9 with R13 and making the timing consistent. In 13.1, 13.2 and 13.3, "when job duties no longer require ..." is ambiguous and should be tied back to the policy of R1.
31.4	Progress Energy - Nuclear Generation	Agree	R13 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
31.5	Minnesota Power	Agree	These criteria are generally acceptable, except for the statement that "Each Registered Entity shall revoke remote access by disabling one or more of the multiple factors required..." The requirement to implement multi-factor authentication is not included in CIP-011-1.
31.6	Independent Electricity System Operator	Disagree	- There is no requirement for removing external access for cause. Does R9.1 cover this access? Should for cause be changed to involuntarily terminated to include those that are terminated unwillingly due to layoffs, job cuts, fired/performance, etc.- R1
31.7	PacifiCorp	Disagree	: The list of criteria is inconsistent with BES system access as outlined in Table 9. Remote access to BES should follow the same revocation criteria as system access.
31.8	USACE - Omaha Anchor	Disagree	13.1 - '... when job duties no longer require remote access' should either be changed 'when terminated for cause' or if the verbiage is deemed appropriate then the length of time to change the password needs to be greatly expanded. Just because an employee changes jobs does not mean they are a threat to the system, they still have the appropriate clearances and training.13.2 & 13.3 - since we are talking about a current employee who is just changing jobs the high impact numbers are crazy. The person is not a threat to the system, they have the necessary background.

#	Organization	Yes or No	Question 31 Comment
			Recommend times be the same as medium impact system.
31.9	Xcel Energy	Disagree	A 1 hour revocation time in R13.1 is completely unworkable. Examples where this is impossible include a termination by a vendor or joint access partner, or a termination during evening hours or weekends/holidays, when IT staff needed to terminate the access can not respond within 1 hour. The 4 and 6 hour revocation times for job duty changes are unjustified and unneeded. When the change is for a business reason such as a job change 7 days is sufficient for access removal. When the access change is unrelated to a termination for cause, the individual's trustworthiness and reliability are not in question and the short timeframes are not warranted.
31.10	BCTC	Disagree	Â Suggest collapsing Requirements 13.1 to 13.3 into one.Â Time targets would be the same as those suggested in Requirement 9 above
31.11	Alberta Electric System Operator	Disagree	Are the "multiple factors" referenced in R13 defined?
31.12	Tenaska	Disagree	Combine 12 and 13
31.13	BGE	Disagree	Combine 13.1, 13.2 and 13.3 into one requirement. Revocation for high impacted systems should be 24 hours to maintain consistency with other requirements with CIP-011.
31.14	Entergy	Disagree	Consider eliminating R13 altogether or combining it with R8.4 and R8.5.Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance perspective to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
31.15	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access. Revocation of remote access within one hour for Control Centers is unreasonable for high-impact

#	Organization	Yes or No	Question 31 Comment
			Systems when the revocation is unrelated to termination with cause. If revocation is the result of one's job duties no longer requiring access, then E ON U.S. suggests next-business day should be adequate. Likewise, six hours for Transmission substation systems, and four hours for Generation Systems is unreasonable. Next business-day revocation should be adequate for all of these situations and presents little, if any, additional risk. E.ON U.S. requests clarification as to what is included in the term "multiple factors" for remote access.
31.16	EEI	Disagree	EEI suggests the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.17	Constellation Energy Control and Dispatch, LLC	Disagree	-Eliminate the timing differences for revoking access when no longer required that exists between Control Centers, generation or transmission facilities and use a single timing requirment for access to all BES cyber systems.-The previous requirements have
31.18	FirstEnergy Corporation	Disagree	For 13.1, 13.2, 13.3 - Change text to '...when job responsibilities no longer requires BES Cyber System remote access'.This table should include a consideration when termination for cause. Should parallel Table 9 expectations.The recommended times are unreasonable for transfers/job reassignments.We have the same concerns with inconsistent application in regards to Impact Level as we previously identified in Table 9. See our comments to Questions 22 and 23.
31.19	Exelon Corporation	Disagree	Implementing revocation of access in as short a time as those proposed would require major changes to many enterprise wide systems in order to document compliance. Why do these time periods differ from those for physical and electronic access? Exelon feels these requirements are too restrictive and might necessitate moving to a 24/7 position to monitor the need for access revocation. Exelon's position is that the

#	Organization	Yes or No	Question 31 Comment
			access revocation should remain at the 24 hours with cause and 7 days without cause. This would also keep the CIP requirements in alignment with the DHS Catalog of Control Systems Security requirement 2.34 - Personnel Termination and DHS Catalog of Control Systems Security requirement 2.35 - Personnel Transfer.
31.20	USACE HQ	Disagree	It does not make sense to create three (3) separate requirements for three specific environments only, I suggest to have only one requirement that reads “Revoke remote access when job duties no longer require BES Cyber System remote access”.
31.21	APPA Task Force	Disagree	New: R13 Table 13.1: For personnel terminated for cause on a preplanned basis. Low Impact: N/AMedium Impact: 8 hourHigh Impact: 8 hourThe Existing 13.1 - 13.3 will need to be renumbered if this new 13.1 is accepted.
31.22	National Grid	Disagree	o National Grid recommends changing from “Required for external connectivity only” to “Required” under High Impact BES CS since the criteria already limits the scope to “remote access” o Reword “remote access” as “Remote access (LAN and wireless) communication interface o 24 hours is the minimal practical time for revoking access. A 1 or 4 hour revocation of access is not reasonable. National Grid suggests keeping times same as in Table R9.
31.23	NextEra Energy Corporate Compliance	Disagree	Please refer to comments submitted for questions 22 and 23. Furthermore, NextEra believes the timeframes suggested will be burdensome to administer since personnel that have authorized remote access have by definition also authorized electronic access. With this current draft, it connotes that when revoking access to High Impact Control Center BES Cyber Systems when job duties no longer require BES Cyber System remote access; the Responsible Entity has 1 hour to revoke remote access per 13.1 and has 36 hours to revoke electronic access per 9.2. We suggest making the time requirements consistent and up date the timeframe to "as soon a practical but within 36 hours" for both 13.1 and 9.2
31.24	Dominion Resources	Disagree	Please see Dominion’s response to Questions 15 and 22. Dominion also requests that

#	Organization	Yes or No	Question 31 Comment
	Services, Inc.		the removal of authentication needed for remote access suffice to meet the intention of this requirement for "immediate" revocation.
31.25	American Electric Power	Disagree	Please see response to Question 32 for additional detail.
31.26	Puget Sound Energy	Disagree	Puget Sound Energy disagrees with the current wording of the criteria. "...when job duties no longer require BES Cyber System remote access" is an abstract concept that will be impossible to quantify in order to validate compliance with the requirement. Puget Sound Energy suggests rewording to "Revoke remote access to...BES Cyber Systems when notification by personnel that job duties no longer require BES Cyber System remote access. In light of the 4 hr to 72 hr clock to revoke access, Puget Sound Energy suggests some measurable trigger from which to start the countdown to required revocation timeframes.
31.27	Detroit Edison	Disagree	R11, R12 and R14 use term "remote electronic access" and R13 uses the term "remote access". Revise to maintain consistency.
31.28	LCEC	Disagree	R13 requirements should be moved to the account management section.
31.29	Southwest Power Pool Regional Entity	Disagree	R13: The objective states that access will be revoked by disabling one or more of the multiple factors required for such access, yet multiple factor access authentication has yet to be prescribed. 13.1, 13.2, and 13.3 simply states "revoke access." As stated, the requirement is unclear and inconsistent between the object statement (Requirement) and the criteria. It may be beneficial to swap Requirements 13 and 14, prescribing remote access authentication controls before prescribing revocation of such access.
31.30	Hydro One	Disagree	Recommend using the same thresholds as R9.Recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope to "remote access".Recommend moving this Requirement to the Boundary Protection Requirements.

#	Organization	Yes or No	Question 31 Comment
31.31	Northeast Power Coordinating Council	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.Recommend moving this Requirement to the Boundary Protection Requirements.
31.32	ISO New England Inc	Disagree	Recommend using the same thresholds as R9Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”Recommend moving this Requirement to the Boundary Protection RequirementsR13.1, R13.2 and R13.3 Is the 36 hours or 72 hours from the time the access is reviewed? Or is it that access should be reviewed within 36 hours of personnel that change job responsibilities, transfer, etc. Then require access be modified based on the review. Suggest changing the 36 hours to 72 hours. If a transfer were to occur on a Friday at 5 pm then access would need to be reviewed by Sunday. R13.1, R13.2 and R13.3 suggest changing the requirement to “Review access to BES Cyber Systems for personnel that change job responsibilities as a result of reassignment, transferred to other positions within x hours of the change.”
31.33	Black Hills Corporation	Disagree	Remote access revocation should be no different that other types of access and the 24 hour should apply.
31.34	Regulatory Compliance	Disagree	Remove R13 altogether and treat revocation of remote access the same as system access.
31.35	Garland Power and Light	Disagree	Requirement 13.1 - Medium Impact should read 48 hours instead of 36 hours and High Impact should read 4 hours instead of 1 hour. To be as strict as written is not necessary for just a job duty change
31.36	Reliability & Compliance Group	Disagree	Revocation for employees terminated for cause needs to be included.

#	Organization	Yes or No	Question 31 Comment
31.37	Southern California Edison Company	Disagree	SCE recommends matching R13 with R9. The time limits for high-impact generation BES is less than transmission substation BES, whereas they are the same in R9. SCE also suggest that 13.2 and 13.3 be given the same time limit.Also, SCE requests clarification about the types of devices that must be revoked. Order 706 seeks immediate revocation to devices and facilities. While order 706 has been unequivocal in the requirement of this control, they do not specify that access to “each” device must be individually revoked. The drafting team should be asked to provide supplemental guidance with this requirement to state that immediate revocation in timeframes shorter than 24 hours to “boundaries” electronic and physical be instituted.
31.38	SCE&G	Disagree	SDT needs to account for transitional periods when incumbent needs to train a replacement for job tasks. In this case when would time period begin for "no longer requiring access". There would be no timestamped document to start the clock.
31.39	ERCOT ISO	Disagree	Should be combined with other access management requirements (physical, cyber, information).
31.40	Manitoba Hydro	Disagree	Since Requirement R13 refers to external access, the words “for external connectivity only” are unnecessary in the impact columns. Please clarify if the “one or more of the multiple factors required for such remote access...” refers to the electronic access controls in Requirement R14. Please clarify what “such access” means.
31.41	Alliant Energy	Disagree	Specifically 1 hour system access removal is not even possible in an environment that is largely automated and unreasonably creates an environment of non-compliance. More generally, Table 13 is another occurrence where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the

#	Organization	Yes or No	Question 31 Comment
			business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
31.42	Allegheny Energy Supply	Disagree	Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.43	Allegheny Power	Disagree	Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems."
31.44	Duke Energy	Disagree	Table 13: How will this apply in case of a death?13.1 change 36 hours to 48 hours
31.45	MidAmerican Energy Company	Disagree	The list of criteria is inconsistent with BES system access as outlined in Table 9. Remote access to BES should follow the same revocation criteria as system access.
31.46	Ameren	Disagree	The short period of time to remove access does not extend well across weekends or through the 2nd business day in cases where access is no longer required at the end of the day. Suggest that these requirements be extended to a week to remain in line with current CIP standards. This will allow for proper hand off time in cases where job duties need to be transferred.
31.47	Southern Company	Disagree	The time limits in 13.1 are needlessly short in the context of an employee who is not

#	Organization	Yes or No	Question 31 Comment
			being dismissed for cause but is simply having his job duties changed. In addition, it is not clear exactly what the trigger point is for the start of that time table.
31.48	Northeast Utilities	Disagree	The timeframe is extreme for routine personnel changes (1 - 6 hours). Suggest a "for cause" termination for these timeframes and make routine more reasonable (3 days to align with R9?) Also, it is not needed if you agree with comment to 29. Host/application and network access should be treated the same.
31.49	Dairyland Power Cooperative	Disagree	These rules seem redundant to table R9. Why are there redundant rules for remote access accounts vs regular accounts? Any rules here should be for something that is unique to remote access.
31.50	US Bureau of Reclamation	Disagree	This requirement appears to be in conflict with R9. In reading R9 it is not clear that it does not also include remote access. Just as in R11 remote needs to be defined especially since R9 does not indicate remote access is excluded as this standards implies. Further, requirements need to be established for all system impact levels and timeframes need to be realistic and achievable. Shorter timeframes, as established in the table, would appear to be more applicable to individuals terminated for cause.
31.51	Consultant	Disagree	This requirement is access revocation and should be included in R9 as it relates to account management and access revocation.13.1, 13.2, & 13.3 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.13.1, 13.2, & 13.3 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.Suggest deleting "for external connectivity only" as redundant & unnecessary. This requirement is for remote access and is by definition external access.

#	Organization	Yes or No	Question 31 Comment
31.52	Bonneville Power Administration	Disagree	This requirement is not necessary. It is already covered under R9. Revocation of electronic access applies to all electronic access regardless of whether it is local, remote or wireless. There is no difference.If the Requirement is retained, then the objective of this requirement ("to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the Requirement rather than appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.
31.53	Progress Energy (non-Nuclear)	Disagree	This revocation is not based on termination for cause. It will be very difficult to meet the 1 - 6 hour revocations. If termination was for cause would an individual not need physical access to get remote access - we are required to physically secure areas around remote access? Shouldn't all access, system, physical, remove etc. have consistent revocation times?Revocation of access within a 'hours' timeframe implies that the access would be controlled through a security group with 24/7 coverage.This should be no different than the revocation of cyber access. This requirement is not needed. Also the time limits as proposed for High Impact are impractical and will only lead to unnecessary self-reports that provide no benefit to system security.CIP-011 R13.1 thru .3 What is the decision process to be used to determine "when job duties no longer require ... access"? What would be suitable compliance evidence that is to be collected that indicates "when job duties no longer require access" as this is critical in determining if revocation has been accomplished within the mandated 1 hour, 4 hours, 6 hours, 24 hours, 36 hours, 72 hours?The complexity and compliance risk of managing all of these requirements at different levels, for different functional areas will be very problematic to substantiate compliance.
31.54	CWLP Electric Transmission, Distribution and	Disagree	Time frames should be extended to 72 hours or next business day, whichever is longer.

#	Organization	Yes or No	Question 31 Comment
	Operations Department		
31.55	Con Edison of New York	Disagree	Timeliness of access removal is important. These criteria can be interpreted (R13.1 for example) to mean remote access needs to be revoked within 7 hours of the actual time of change of job duties. This can be unrealistic. The controlling department, for access, may not be notified by the individuals department of the change within the time period. This is more likely when contract personnel are considered. The requirement should be clearly worded to provide 7 hours from notification of the need for change.R13.2 and 13.3: it is not clear that the standard defines either a Transmission or Generation BES Cyber System.
31.56	We Energies	Disagree	We Energies agrees with EEI: Suggest the following revision:"Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 - Remote Access Revocation to prevent unauthorized operation of BES Elements by maintaining control of access to its BES Cyber Systems." We Energies agrees with EEI: Suggest adding requirements to address the removal of remote access for low impact systems.
31.57	GTC & GSOC	Disagree	We recommend this requirement include language that would allow personnel to retain access during a transition period while training their replacement. We recommend the language used in requirement 5, row 5.8: "personnel who no longer require such access."We also recommend that termination for cause should be handled seperately. All other time lines should be commensurate with the associated risk and consistent throughout all requirements.We recommend the language in Table 13 should be consistent with 5.8 and 5.9 in Table 5.We recommend requirements 13.1, 13.2, 13.3 should include the words "the entity determines the" between the words "when" and "job"; this would prevent an auditor from second guessing an entity's decision on required access. The requirement should also specifically state that this does not preclude a person from retaining access in order to assist his replacement with fulfilling his old job duties during a transition of

#	Organization	Yes or No	Question 31 Comment
			responsibilities.
31.58	Network & Security Technologies Inc	Disagree	Wording suggests multi-factor authentication is required for all systems subject of R13, but R14 only requires multiple factors for High Impact systems. Also suggest swapping order of requirements in R13 and R14.

32. Table R13 provides direction concerning what impact level of BES Cyber Systems to which Requirement R13 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R13 has moved to CIP-004-5 – Cyber Security - Personnel and Training, Requirement R5.

Commenters suggested aligning with R9 normal revocations. In response, the requirements for revocation have been consolidated to CIP-004-5 R7.

Commenters suggested including targets for Low Impact BES Cyber System revocation. The SDT notes the applicability to Low Impact BES Cyber Systems has been removed.

Commenters suggested times need to be stated in business days. In response, times have been changed to calendar days. The use of business days is not appropriate because this can be interpreted to include exclusions for weekends and holidays.

#	Organization	Yes or No	Question 32 Comment
32.1	Luminant	Agree	13.1 should be changed to 48 hours (2 days)
32.2	USACE - Omaha Anchor	Agree	Agree - just want to reiterate the times associated with removal for a job transfer are ridiculous. The person has been trusted and trained - it's not an emergency just because they changed jobs. (Due to lack of personnel - if this happened on a Friday - we would have to treat it as an emergency.)
32.3	Idaho Power Company	Agree	Need to make this consistent with revocation requirements for normal electronic access. Why would these timelines be shorter?
32.4	SCE&G	Agree	The timeframes, specifically for High Impact Control Center assets, are extreme.
32.5	US Army Corps of Engineers, Omaha Distirc	Disagree	"when job duties no longer require" will be very hard to account for. Time frames are unrealistic / impossible. Times should be stated in terms of business days. It would be more realistic for High Impact BES Cyber Systems to be Next Business Day and for Medium Impact Cyber Systems to be 2 and 3 business days.

#	Organization	Yes or No	Question 32 Comment
32.6	Florida Municipal Power Agency	Disagree	1 hour is not reasonable. Planned termination for cause can be 1 hour, but, otherwise the 1 hour is not reasonable. Consider aligning the times with R5 and R9. Access revocation alternatives/mitigation techniques should allow for deviation from the standard, or be recognized. For example, escorted supervision while restricting access to communication devices/computers should be a reasonable way to get around the 1-hour requirement if it can't be met for some particular reason.
32.7	American Electric Power	Disagree	13.1 - 13.3, regarding all information in column "High Impact BES Cyber System". These values are not feasible on a system unless it is managed with a domain controller or has only a few network components. Suggest using the 36/72/72 as required in the R9. There is no need to make this more restricted than the local access.There also does not appear to be a requirement to revoke access within 24 hours for a termination for cause. Is that the intent?
32.8	Con Edison of New York	Disagree	13.1,2,3- may be dependent on a company's existing HR/Payroll business system capabilities and introduce significant costs to remediate. Even though the individuals were trusted and the trust did not change as a result of cause. A week may be more realistic
32.9	ERCOT ISO	Disagree	13.1: 1 hour may not be possible. Especially in light of access granted to external organizations (ie: an RC or BA with access a TOP's systems).
32.10	Southern California Edison Company	Disagree	A longer time frame (range of <72 hours for high medium and low impact systems) should be instituted for each device. Revocation should not be treated as a monolithic requirement and should be such that it leverages controls instituted by boundary protections.
32.11	Constellation Energy Commodities Group Inc.	Disagree	Align all high and medium impact systems on the 72 hour standard to eliminate confusion and allow consistent administration.

#	Organization	Yes or No	Question 32 Comment
32.12	MidAmerican Energy Company	Disagree	As noted in question 31 we believe that the list of criteria should align with Table 9, the impact levels should begin with termination for cause and then address the criteria. In addition, the impact between transmission and generation is inconsistent and not understood why these would be different, again inconsistent with Table 9. With regards to the impact levels - time to revoke access - we disagree that this too would be different than as outlined in Table 9. All revocation requirements under 24 hours is concerning as this imposes significant risk to our ability to comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.
32.13	PacifiCorp	Disagree	As noted in question 31 we believe that the list of criteria should align with Table 9, the impact levels should begin with termination for cause and then address the criteria. In addition, the impact between transmission and generation is inconsistent and it is not understood clear why these would be different, again inconsistent with Table 9. With regards to the impact levels - time to revoke access - we disagree that this too would be different than as outlined in Table 9. All revocation requirements under 24 hours is concerning as this imposes significant risk difficulty to our ability to comply given the lack of available automated access removal solutions in the market place that can be realistically deployed across a wide-range of systems.
32.14	American Transmission Company	Disagree	As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.15	MRO's NERC Standards Review Subcommittee	Disagree	As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-

#	Organization	Yes or No	Question 32 Comment
			compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.16	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
32.17	Tenaska	Disagree	Combine 14 and 11
32.18	The Empire District Electric Company	Disagree	Comments: As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.
32.19	Alberta Electric System Operator	Disagree	Consider adding “120 hours for external connectivity only” to all Low Impact BES Cyber System levels (13.1, 13.2, 13.3).
32.20	Entergy	Disagree	Consider eliminating R13 altogether or combining it with R8.4 and R8.5.Suggest combining 9.2 thru 9.4 and making all 72 hours. CIPv1 is very prescriptive in this area. It is easier from a compliance perspective to have a 24 hour revocation requirement for termination and 72 hour requirement for everything else.
32.21	Duke Energy	Disagree	Drafting team, please explain the basis for the 1 hour, 6 hour, and 4 hour requirements for the High Impact column. These appear to be overly restrictive and arbitrary. Similar to the comment above, these items are much more achievable if "remote" and "external" are defined as external to the plant in a generation

#	Organization	Yes or No	Question 32 Comment
			environment. Also, as stated above (question 27), remote connectivity requires more unambiguous definition.
32.22	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access
32.23	USACE HQ	Disagree	First, requirements 13.1, 13.2, and 13.3 should be required for every level of impact. Second, to avoid the "Friday 5PM no longer required access" scenario, the language should be change as follow: for High Impact BES Cyber System in 13.1, 13.2, and 13.3, from "XX hours for external connectivity only" to "Close of Business Day (COB) of the following day after the no longer access required for external connectivity only", for Medium Impact BES Cyber System in 13.1, 13.2, and 13.3, from "XX hours for external connectivity only" to "Close of Business Day (COB) of the second day after the no longer access required for external connectivity only", and for Low Impact BES Cyber System in 13.1, 13.2, and 13.3 (please refered to my answer to question 31), from "----" to "Close of Business Day (COB) of the third day after the no longer access required for external connectivity only".
32.24	Network & Security Technologies Inc	Disagree	If authentication is required for remote access to Low Impact systems (R14), it should be covered by R13 revocation.
32.25	WECC	Disagree	If the employee can access the system remotely why can the entity not remotely disable the access? Please have another look at the hours for the medium impact level.This should apply to all impact levels and Medium and Low impact systems should require not more than 24 hour timelines for revocation.
32.26	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
32.27	BGE	Disagree	Low impacted systems should have a timeframe defined for revocation

#	Organization	Yes or No	Question 32 Comment
32.28	FirstEnergy Corporation	Disagree	Need clarity on '...for external connectivity...'. For example, does this mean consoled in (directly connected) as well as remote electronic logon?Timeframes should not be in 'hours' (i.e. less than a full day). Tracking by time rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities.Similar concerns as previously stated with Table 9. See Questions 22 and 23.
32.29	Detroit Edison	Disagree	Please explain the reason for different revocation times between High Impact on 13.2 and 13.3.
32.30	American Municipal Power	Disagree	Please provide a little or no impact category
32.31	NextEra Energy Corporate Compliance	Disagree	Please refer to comments submitted for questions 22 and 23.
32.32	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12 and Table 13. Puget Sound Energy suggests including wording similar to Table 11: "Required for external connectivity only".
32.33	Progress Energy - Nuclear Generation	Disagree	R13 durations should align with those described in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
32.34	LCEC	Disagree	R13 requirements should be moved to the account management section.
32.35	ISO New England Inc	Disagree	Recommend using the same thresholds as R9 Recommend changing from "Required for external connectivity only" to "Required" since the criteria already limit the scope

#	Organization	Yes or No	Question 32 Comment
			to “remote access”
32.36	Hydro One	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
32.37	Northeast Power Coordinating Council	Disagree	Recommend using the same thresholds as R9.Recommend changing from “Required for external connectivity only” to “Required” since the criteria already limit the scope to “remote access”.
32.38	Black Hills Corporation	Disagree	Remote access revocation should be no different that other types of access and the 24 hour should apply.
32.39	Public Service Enterprise Group companies	Disagree	Remote access should be governed by the same rules are normal access. The time frame in 13.1 for High Impact BES Cyber Systems is unreasonably short. Notifying and securing the appropriate personnel to disable access once the job duties no longer require access may not be possible in all circumstances to guarantee that access is always revoked within 1 hour. This may not be operationally feasible. The timeframe should be similar to access revocation for user with non-remote access as specified in Table R9 item 1.9 (i.e. within 24hrs).
32.40	Manitoba Hydro	Disagree	Remote electronic access to BES Cyber Systems should be revoked for Low Impact BES Cyber Systems, and not permitted indefinitely. The remote access revocation period for generation High Impact BES Cyber Systems should be 6 hours, the same as for the Transmission High Impact BES Cyber System.
32.41	Exelon Corporation	Disagree	Requirements 13.1, 13.2 and 13.3 contain time parameters in hours. Exelon’s tracking systems that would be used to demonstrate compliance are tracked in time increments of days, not hours. If an hourly timeframe is required it will cause extensive modifications to numerous enterprise wide systems to allow tracking at an hourly level. One must ask how this improves reliability. What is the basis for time

#	Organization	Yes or No	Question 32 Comment
			levels and having a different timeframe for a control center than other locations? With the exception of a termination for cause, what is the basis for requiring access removal for someone who was a trusted employee on such an aggressive timeframe? What is the risk that is being addressed by making a 1 hour timeframe requirement?
32.42	Southwest Power Pool Regional Entity	Disagree	Revocation timeframes should be expressed in business days.
32.43	National Grid	Disagree	Same as in Q. 31.
32.44	San Diego Gas and Electric Co.	Disagree	SDG&E feels that the key for this requirement is the definition of the phrase "when job duties no longer require remote access". This phrase can be interpreted in a couple of different ways. The more strict interpretation is that a person would no longer need access after their session is complete, or perhaps after taking a break or going to lunch. This could happen a few times per day, depending on the work. A second interpretation could mean that a person no longer needs access after a 6 month long project is completed or there is a reassignment to another part of the company after 3 years of working on the BES Cyber Systems, etc. In the former case, it becomes a large burden to revoke access within one hour several times per day, and could be a manual process on some systems. On the other hand, if you consider the second interpretation (6 month project or transfer after 3 years), SDG&E would ask why is it so important to revoke remote access with 1, 4, or 6 hours after such a long period of time that a person has had access? Sometimes it takes time for a person to get reassigned, change locations, change projects, etc. In this case, 4 hours would be the minimum that SDG&E feels is practical to be able to comply with.
32.45	Progress Energy (non-Nuclear)	Disagree	See comment 14.This should be no different than the revocation of cyber access revocation. This requirement is not needed.
32.46	GTC & GSOC	Disagree	See comments to question 31 above

#	Organization	Yes or No	Question 32 Comment
32.47	BCTC	Disagree	See our response for table 9 time targets
32.48	Constellation Energy Control and Dispatch, LLC	Disagree	See response to Question 31.
32.49	Regulatory Compliance	Disagree	STRIKE Table R13
32.50	EEI	Disagree	Suggest removal of the words “for external connectivity only” from the table 13 columns, as the requirement themselves discuss the issue of remote access, therefore the words “for external connectivity only” are unnecessary and redundant.EEI suggests using a uniform number of hours across various facility types for high and medium.EEI suggests using 7 calendar days for medium.EEI suggests using 8 hours for high impact.EEI suggests adding a footnote here to reference the definition put forth in R11: “Remote access for the purpose of this standard means an interactive user session with a BES Cyber System from a device external to the BES Cyber System.”
32.51	Allegheny Energy Supply	Disagree	Suggest using a uniform number of hours across various facility types for high, medium and low.Suggest using 7 calendar days for medium and 14 calendar days for low impact.Suggest using 12 hours for high impact.
32.52	Allegheny Power	Disagree	Suggest using a uniform number of hours across various facility types for high, medium and low.Suggest using 7 calendar days for medium and 14 calendar days for low impact.Suggest using 12 hours for high impact.
32.53	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS comments noting that as written, the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access). However we feel the one area where an entity is vulnerable is when personnel are terminated for cause. We see this as the most extreme case when an

#	Organization	Yes or No	Question 32 Comment
			entity should be diligent in protecting remotely accessible BES cyber systems and act within the time of a normal shift. We suggest 8 hours for termination for cause, except when a termination is preplanned, in which case a shorter time period may be feasible. Similar to the comments we provided regarding R9: We know there are pressures to have access restricted as soon as possible but we are trying to be realistic given the time it will take to remove access from systems which have multiple owners, are in remote locations and which have numerous devices to access. It seems that the drafting team is basing their proposed timetable on a control center where the cyber systems are more IT focused and have controls that can be turned on and off easily.We propose the following changes to the Impact Levels of R13:R13 Table 13.1: (NEW) Low Impact: N/AMedium Impact: 8 hoursHigh Impact: 8 hoursR13 Table 13.2: (Old 13.1)Low Impact: N/AMedium Impact: 36 hoursHigh Impact: 36 hourR13 Table 13.3: (Old 13.2)Low Impact: N/AMedium Impact: 1 WeekHigh Impact: 1 WeekR13 Table 13.4: (Old 13.3)Low Impact: N/AMedium Impact: 1 WeekHigh Impact: 1 Week
32.54	Minnesota Power	Disagree	The impact levels seem well defined however inconsistencies in the definitions of “remote access” and “external connectivity,” (see response in Question 26) create confusion regarding the applicability of the criteria for each impact level.In certain circumstances, it may not be possible to adhere to the proposed timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week or where notification of termination comes from corporate systems that are also updated on an 8 hours a day, 5 days a week schedule. The need for more immediate time constraints, when compared to electronic access as defined in Requirement R9 that is not remote is understood, but both the Requirements in R9 and R13 need to take into account reasonable business processes that impact notification of employee reassignment and separation.Minnesota Power recommends that the timelines for R13 be consistent with those established in R5 and R9, but would agree that terminology should be included urging Registered Entities to expedite this process as much as possible with regards to remote access.

#	Organization	Yes or No	Question 32 Comment
32.55	GE Energy	Disagree	The revocation targets for High Impact systems will be almost impossible to meet for revoking vendor personnel access (Table R13 HI BES remote access must be terminated within 1 hour of access no longer being required). It also seems to be in conflict with the revocation times in Table R9? These need to be linked together.
32.56	Northeast Utilities	Disagree	The timeframe is extreme for routine personnel changes (1 - 6 hours). Suggest a "for cause" termination for these timeframes and make routine more reasonable (3 days to align with R9?) Also, it is not needed if you agree with comment to 29. Host/application and network access should be treated the same.
32.57	US Bureau of Reclamation	Disagree	The timeframes for High Impact are not consistent with R9 and appear to be too stringent. Further, requirements need to be established for all system impact levels.
32.58	Oncor Electric Delivery LLC	Disagree	These proposed time frames are not practical as most HR systems are separate (and should be) from real-time operations of the BES. The time-frames for High Impact cannot be different from Medium, as they utilize the same back-office information systems.
32.59	Bonneville Power Administration	Disagree	These requirements are not necessary. They are already covered under R9. Revocation of electronic access applies to all electronic access regardless of whether it is local, remote or wireless. There is no difference. In addition, this requirement could force Cyber System administrative personnel to take action to revoke access even if it means not performing other actions needed to support real-time operations, or risk non-compliance. As an example, if a BES Cyber System has failed for some reason, the corrective actions should take precedence over revoking access. Under those circumstances, an entity could find itself in the position of deliberately allowing non-compliance in order to restore the integrity of the BES. The required time frames are impossibly short for high impact systems. It is difficult to justify dropping all other actions to revoke access for someone unless there is reason to believe that the individual poses a threat. In that case the requirements of R9 are in effect.This

#	Organization	Yes or No	Question 32 Comment
			requirement seems to conflict with R9 and Table R9. Table R9 allows 24 hours for access revocation due to termination for cause. Table requires revocation within 1 hour, even if termination for cause is not required.Recommendation: Remove this requirement entirely. Treat revocation of remote access as just another revocation of access under R9. Otherwise, increase the time frames to something achievable.
32.60	Consultant	Disagree	This requirement is access revocation and should be included in R9 as it relates to account management and access revocation.13.1, 13.2, & 13.3 - Whatever time frame is selected, the revocation time should be stated in days, either working days or calendar days, as personnel transactions typically are not conducted or tracked on an hourly basis.13.1, 13.2, & 13.3 - Having a different time frame for different types of facilities is an added dimension to the impact categorization that should be eliminated. If there is a basis for a difference in revocation times for different facility types, that difference should be included in the impact categorization criteria, not by trying to add additional categorization criteria in the requirements.Suggest deleting "for external connectivity only" as redundant & unnecessary. This requirement is for remote access and is by definition external access.
32.61	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
32.62	We Energies	Disagree	We Energies agrees with EEI: Suggest removal of the words "for external connectivity only" from the table 13 columns, as the requirement themselves discuss the issue of remote access, therefore the words "for external connectivity only" are unnecessary and redundant.We Energies agrees with EEI: Suggest using a uniform number of hours across various facility types for high, medium and low.We Energies agrees with EEI: Suggest using 7 calendar days for medium and 14 calendar days for low impact.We Energies agrees with EEI: Suggest using 8 hours for high impact.We Energies agrees with EEI: Suggest adding a footnote here to reference the definition put forth in R11: "Remote access for the purpose of this standard means an interactive user session

#	Organization	Yes or No	Question 32 Comment
			with a BES Cyber System from a device external to the BES Cyber System.”

33. Requirement R14 of draft CIP-011-1 states "Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to its BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls to ensure that no unauthorized access is allowed to its BES Cyber Systems." Do you agree with the list of criteria that is included in Requirements Table R14? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Requirements for remote access in CIP-011-1 R14 have moved to CIP-005-5 - Cyber Security — Electronic Security Perimeters.

Commenters expressed concern that the scope of the "Banner" requirement should be clarified and that having a banner is not a security control. The SDT agrees and notes that the requirement to have appropriate use banners was considered administrative and has been removed.

Several other commenters suggested splitting wireless and remote access requirements. The SDT notes that a new requirement for Remote Access Management (CIP-005-5 R2) was created based on the Urgent Action Revisions to CIP-005-3, and the wireless access requirements have been removed.

#	Organization	Yes or No	Question 33 Comment
33.1	WECC		Don't see the security value of requiring login banner as required in 14.4. This requirement seems to stem from the belief that in a legal prosecution the court would need to show that the system was misused or accessed inappropriately and that a login banner accomplishes this by notification. Since most attacks are done via automation today, and internal attackers are likely required to sign an acceptable use policy this requirement seems to only add operational cost. Additionally, one can prove that inappropriate use was done by the mere fact that the person is using the system without authorization. Also keeping this in for only high impact systems would let attackers easily know which systems are high impact/value. Recommend dropping criteria all together. The appropriate use banner criterion does not belong here. This is a legal protection, not a security control, and would be better placed in a policy type requirement. Consider replacing "multi-factor" with "strong", and offering

#	Organization	Yes or No	Question 33 Comment
			additional language to clarify the term. "Strong" auth should be required for all remote access. Provide distinction between remote access from untrusted locations, such as the internet, and remote access from trusted locations, such as a backup control center.
33.2	Duke Energy	Agree	14.4 requires a TFE
33.3	Regulatory Compliance	Agree	BUT14.2 - What is the risk protection versus cost, time and overhead to implement?
33.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
33.5	CWLP Electric Transmission, Distribution and Operations Department	Agree	Is multifactor access control limited to electronic methods only? Can the use of enabling or disabling a device such as a modem equal to a portion of multifactor controls?
33.6	Puget Sound Energy	Agree	Puget Sound Energy agrees with the criteria, but suggests NERC provide clarity in regards to 14.4. Is NERC requiring an "appropriate use banner" on the user screen for the initial attempt of remote access, or for all interactive attempts established after successfully authenticating remotely? Example: Is an appropriate use banner only needed for a 2-factor VPN connection screen, or at all systems accessed through a 2-factor VPN (operating system and application(s) on BES Cyber System Components?
33.7	Progress Energy - Nuclear Generation	Agree	R14 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
33.8	GTC & GSOC	Agree	We recommend references to wireless should be removed from R14 and the associated table. The actual requirements are not related to wireless as distinct from

#	Organization	Yes or No	Question 33 Comment
			other remote access
33.9	Green Country Energy	Agree	Will their be guidance? How about changing the statement to "reasonably ensure" that no unauthorized access is allowedExample: If my processes allow anyone to be authorized, I then can "ensure" no unauthorized access will occur.
33.10	Independent Electricity System Operator	Disagree	- R14.1 and R14.2 seem to be stating the same thing. R14.2 is covered by R14.2.- R14.4 - Shouldn't the use banner be required to be installed on the BES cyber components themselves prior to login. If port 22 is open on a firewall, the firewall will
33.11	American Electric Power	Disagree	14.1: Regarding "If remote access is used and/or implemented, include authentication controls". Suggest replacing "include" with "document".
33.12	FirstEnergy Corporation	Disagree	14.2 this could be difficult to implement depending on the definition of "interactive user session" within the definition of remote access.14.2 - add '...authentication controls for remote access mechanisms'14.3 - add 'remote access' somewhere in this sub-requirementWith R14.4, it requires an appropriate use banner; there is no allowance for equipment that can not support a banner.
33.13	Luminant	Disagree	14.4 - where technically feasible
33.14	Southwest Power Pool Regional Entity	Disagree	14.4 is overly prescriptive. Consider revising the requirement to simply state "Display an "appropriate use banner" upon an interactive attempt to access a BES Cyber System, stating that unauthorized use of the system is prohibited."
33.15	BCTC	Disagree	Â R 14.1: remove Required as the requirement is satisfied under R14.2R14.4: text "remote electronic access" devices; suggest that the language be rewritten/ simplified so the objective is clear - i.e. ensure appropriate CCAs display appropriate use banner when connecting to these assets remotely
33.16	Southern California	Disagree	As stated above, remote access should be thoroughly documented and full encryption

#	Organization	Yes or No	Question 33 Comment
	Edison Company		and authentication methods applied.Also, SCE requests that the drafting team review the intent of R14.4 and R7.2 and consider combining the requirements.
33.17	Tenaska	Disagree	Combine 14 and 11
33.18	Alliant Energy	Disagree	Consideration should be given to whether or not the access provides control capability or simply read only.
33.19	ISO New England Inc	Disagree	Did the SDT assume that wireless is a form of remote access for R11 - R14? If YES, please update the wording. If NO, the Requirements are confusing because we use wireless that is not remote access, plus wireless includes more than WiFi.Depending on that answer, R14 should move into R11 or into the Boundary Protection RequirementsR14.1 and R14.2 seem to be stating the same thing.14.2 should have requirement for medium. 14.4 appropriate use banner - is this required for legal steps in the event of an issue... this is not a security control.If the banner is need then the use banner should be required to be installed on the BES cyber components themselves prior to login. If port 22 is open on a firewall, the firewall will allow the traffic through without displaying a banner.
33.20	Northeast Power Coordinating Council	Disagree	Did the SDT assume that wireless is a form of remote access for R11 - R14? If YES, the wording should be revised. If NO, the Requirements are confusing. Wireless that is not remote access may be used, plus wireless includes more than WiFi.Depending on that answer, R14 should move into R11 or into the Boundary Protection Requirements.
33.21	Florida Municipal Power Agency	Disagree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.Item 14.4 is very specific in requiring “appropriate use banner” this should be removed or reworded to cover various methods of notification. Also the standard should demand that no identifiable details be given about the system before authentication is complete.We believe items 14.3 and 14.4 are going to set the stage for numerous TFE’s within the industry. Many devices (e.g.,

#	Organization	Yes or No	Question 33 Comment
			protective relays) do not support explicit access permissions and appropriate use banners.
33.22	USACE - Omaha Anchor	Disagree	Have concerns about 14.2 “multifactor authentication.” Would prefer terms either “multi-authentication.” If we were to implement multifactor we would be removing levels of access to our system and potentially making it easier to hack if they can overcome the multifactor issue.
33.23	Black Hills Corporation	Disagree	If two cyber systems are on the same protected network, and within the same physical boundary, should two-factor authentication be required? We don’t think so, but according to the definition of remote access and this requirement it would be.
33.24	LCEC	Disagree	Is this for remote access and wireless network access or does it also apply to wireless communications between BES Cyber System Components?
33.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes the multifactor controls required in section 14.2 is too specific. “Strong technical controls” is a preferred update to the requirement. There may be better controls from a security and reliability standpoint, but as the requirement stands, Responsible Entities are limited in the technological implementations to support compliance to the requirement.Requirement 14.3 specifying that responsible entities must “deny access by default; [specifying] explicit access permissions” is unclear. Since this is supposed to be related to remote electronic access, the requirement should clarify that the end user is explicitly denied access thru the access point(s) of the network containing the BES Cyber System unless explicitly allowed access into that network.Requirement 14.4 requires the displaying “of an ‘appropriate use banner’ on the user screen of remote electronic access control devices that, upon an interactive attempt to access a BES Cyber System, states that unauthorized use of the system is prohibited.” This appropriate use banner should be required upon every new connection and entry attempt to the BES Cyber System network, for example a firewall or SSL VPN connection that controls remote access. Also, allowance for TFE's in 14.2 through 14.4 should be included.Regarding 14.2, NextEra

#	Organization	Yes or No	Question 33 Comment
			would like clarifaction for the required multifactor authentication controls. Is it required for assets within the boundary or does it only apply to the control of wireless and remote access to electronic access points to BES Cyber Systems? or both?
33.26	Constellation Energy Commodities Group Inc.	Disagree	Provide clarification regarding acceptable use banner (14.4) - in some instances such banners cannot be added to system. Make clear that the requirement may be met by displaying a banner upon workstation sign-on or upon user entry to the remote access environment. What is the specific meaning of authentication controls in 14.1? Since this is called out separately from two-factor authentication, I interpret it to mean that remote access cannot be enabled via generic accounts, only via user specific accounts with authentication (password) known only to the individual. Is that the idea?
33.27	Detroit Edison	Disagree	R11, R12 and R14 use term “remote electronic access” and R13 uses the term “remote access”. Revise to maintain consistency.Wireless electronic access is not an access method; it is just the medium to obtain access. In an effort to remove reference to specific technology, wireless should not be identified anywhere in the standard. References to specific technologies should be addressed in the guidance documentation.
33.28	Ameren	Disagree	R14.1 - The complexity and scope of the documentation of the Low Impact Systems will be challenging to keep succinct for auditors.R14.3 - Deny access by default is not needed. Requiring authentication implies access is denied by default.R14.4 - Not all systems support user banners. This will be hard to keep from being a TFE on many “high” systems.
33.29	Southern Company	Disagree	R14.1-4 addresses remote access only and does not include wireless, the table title and R14 includes wireless.
33.30	Entergy	Disagree	R14.2 dictates multifactor authentication controls for only high impact BES Cyber Systems. Entergy recommends serious consideration of extending this to low and medium impact BES Cyber Systems where localized wireless technology is employed.

#	Organization	Yes or No	Question 33 Comment
			Eliminate 14.4. We understand the purpose of this requirement but do not believe that it adds to the protection of any cyber system. If it is to be added then it should be placed outside of the wireless and remote electronic access control section and placed elsewhere. Entergy believes some aspects of R11 and R14 are redundant and suggests combining them. We also believe criteria in R14 should apply to high, medium and low risk assets and provide a footnote indicating that where requirements are unable to be met explicitly that the strongest possible controls should be employed alternatively.
33.31	US Bureau of Reclamation	Disagree	R14.3: Add deny access by default requirement for low systems. Specific access permissions are not required, however.
33.32	San Diego Gas and Electric Co.	Disagree	SDG&E recommends that a definition of what is meant by “multifactor authentication controls” be included in a definition box near R14.
33.33	APPA Task Force	Disagree	The APPA Task Force agrees with the MRO-NSRS proposal. Criteria in 14.3 and 14.4 are very specific in application of technology that may not be supported by devices in the field. These criteria should be removed or reworded to cover various methods of operation. If the drafting team keeps these requirements the following is our recommended language: R14 Table 14.3: If a BES cyber system component supports explicit access permission capability, the device should deny access by default. R14 Table 14.4: If a BES cyber system component supports notification capability, remote electronic access control device users should be notified that unauthorized use of the system is prohibited.
33.34	MidAmerican Energy Company	Disagree	The new definition of BES Cyber System creates confusion over what technologies are intended to be in-scope. The core changes significantly changes how a responsible entity (RE) establishes and secures remote access to these systems. The REs will develop their own unique determination on how to deal with this situation. Which is likely not going to deliver the intended result the Standards drafters are looking for industry-wide? As this relates to R22 - firewalls, our CIP defined access points, are

#	Organization	Yes or No	Question 33 Comment
			defined as part of a given BES Cyber System. One likely scenario is that we will define a separate BES Cyber System that manages these firewalls that might include a client PC, a firewall manager, and some network infrastructure components. The remote access rules and even the other general protections of these cyber components to manage this type of communication become very ambiguous.Retain the existing ESP concept versus adopting the BES Cyber system concept and make some of the other operational improvements this draft makes.While the criteria themselves are not onerous for the long term/future development of the systems, the current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.
33.35	PacifiCorp	Disagree	The new definition of BES Cyber System creates confusion over what technologies are intended to be in- scope. The core changes significantly changes how a responsible entity (RE) establishes and secures remote access to these systems. The REs will develop their own unique determination on how to deal with this situation. Which is likely not going to deliver the intended result the Standards drafters are looking for industry-wide? As this relates to R22 - firewalls, our CIP defined access points, are defined as part of a given BES Cyber System. One likely scenario is that we will define a separate BES Cyber System that manages these firewalls that might include a client PC, a firewall manager, and some network infrastructure components. The remote access rules and even the other general protections of these cyber components to manage this type of communication become very ambiguous.Retain the existing ESP concept versus adopting the BES Cyber system concept and make some of the other operational improvements this draft makes.While the criteria themselves are not onerous for the long term/future development of the systems, the current BES technology in place or available, will require technical feasibility exceptions as not all systems within the BES can support all criteria listed.
33.36	Bonneville Power Administration	Disagree	The objective of this requirement (‘to ensure that no unauthorized access is allowed to its BES Cyber System”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than

#	Organization	Yes or No	Question 33 Comment
			appearing at the end of the Requirement (i.e., the text of the Requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In addition: Table R14, Section 14.2 is excessive. Given the draft Standard's definition of external connectivity, remote access could also be a case of accessing a system from a nearby system over secured communications paths. An example would be a user on one BES Cyber System accessing another BES Cyber System in the same Control Center. It is not reasonable to justify multi-factor authentication in these circumstances. In addition, many existing systems do not have the capability of enforcing multi-factor authentication. Finally, there are other authentication controls stronger than username/password which are not multifactor: biometric, one time passwords, dial-back, and so forth. Recommendation: Delete the requirement. If not, change the definition of "external connectivity" as discussed in question 13, and change the requirement from "multifactor authentication controls" to "authentication controls stronger than username/password".Section 14.4. There are significant issues with this requirement. - The warning banner is a legal requirement, not a security requirement. Its only purpose is to provide support for legal recourse if someone violates what it says. - No unauthorized person should be accessing High Impact Cyber Systems. Any user with authorized electronic access will have completed security training, which includes proper use of BES Cyber Systems. Any unauthorized user will ignore the banner. - It does not prevent unauthorized access, and therefore does not support the purpose of the requirement. - The requirement has technical feasibility issues. To provide specific scenarios: 1. The user connects from a device controlled by the Responsible Entity, using networks owned by the RE. The user authenticates at the local device. When attempting to connect the the BES Cyber System, the firewall access point allows the traffic, based on the originating point within the trusted network. The user again authenticates at the BES CYber System. At no time does the user authenticate at the access point itself (nor does the rest of Table R14 require authentication at the access point.) In fact, under these circumstances firewalls generally do not have the capability to request authentication or present a banner. 2. The user connects via a

#	Organization	Yes or No	Question 33 Comment
			VPN. The VPN client authenticates the user, then uses a PKI certificate to authenticate to the access point. The user is then granted access to the network and can proceed to authenticate and connect to a BES Cyber System. At no point did the user authenticate to the access point, nor was there an opportunity to present a banner.Recommendation: The best solution is to eliminate the requirement. If the requirement cannot be removed:First, change the definition of remote access and/or external connectivity as discussed above. This would eliminate the requirement to present a banner to users attempting access from equipment belonging to the Responsible Entity. Second, allow the banner to be present at locations other than the access point. A possible revised requirement would be: "Display an "appropriate use banner" to the user that, upon an interactive attempt ..." Also, change "Required" to "Required for external connectivity only".
33.37	Consultant	Disagree	The terminology "wireless and remote access" is redundant. The definition of remote access (near requirement R11) includes wireless access implicitly. Suggest using the defined term "Remote Access" rather the redundant terminology.Table R14 - Item 14.1 It seems illogical to require authentication controls on Low Impact systems when there is no Account Management required for these systems. Suggest deleting the requirement for Low Impact BES Cyber Systems.Items 14.1 & 14.2 - The terminology "is used and/or implemented" seems redundant. It appears that being "implemented" creates the vulnerability, and the requirement for control. Suggest changing the words "is used and/or implemented" to "is implemented".Item 14.3 - This includes two different requirements: (1) Deny access by default & (2) specify explicit access permissions. The first requirement is a technical implementation and should remain here. The second is an account management requirement and should be moved to the account managment requirement R8.
33.38	Minnesota Power	Disagree	These criteria are generally acceptable; however, Minnesota Power requests that the Standards Drafting Team consider defining “authentication controls.”Also in Part 14.2, the requirement regarding the use of multifactor authentication controls sets a technology-specific direction that may not stand over time, including the possibility of

#	Organization	Yes or No	Question 33 Comment
			biometric authentication that, while not multifactor, is a stronger control.
33.39	Dominion Resources Services, Inc.	Disagree	To avoid the potential for TFE's associated with R14.4, a footnote similar to the one used for Table R10 on Page 11 of CIP-011 should be added. Also, access controls related to access points would be better addressed in the Boundary Controls Section of CIP-011.
33.40	Hydro One	Disagree	We don't understand the emphasis on wireless communication and believe that in the present form, it would be very complex to implement. It's our opinion that the protection should remain the same regardless of the type of access point.
33.41	Progress Energy (non-Nuclear)	Disagree	What conditions would dictate different authentication controls for different impact levels? Is it better for them to all be the same?R14.4 is unnecessary. The population of persons granted remote access rights is extremely limited and these people are highly trained and trustworthy. The appropriate use banner is used in situations where a general population was granted this type of access and that is not the case for remote access to any control systems.
33.42	National Grid	Disagree	What types of authentication controls are valid? (Authentication level such as a shared password or a user level control)
33.43	Alberta Electric System Operator	Disagree	Wireless access and remote access should be two separate concepts.
33.44	Network & Security Technologies Inc	Disagree	Wording of 14.4 gives the (doubtless unintended) impression a banner must be displayed on the user screen of electronic access control devices. Re-word to clarify banner must be displayed on the user screen of the accessing device.

34. Table R14 provides direction concerning what impact level of BES Cyber Systems to which Requirement R14 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 R14 has moved to CIP-005-5 R1.

Commenters expressed that the 'deny by default' requirement should also apply to Low impact BES Cyber Systems. In response, the SDT agrees that some network access control should apply to all BES Cyber Systems, including the Low Impact BES Cyber Systems. CIP-005-5 R1 – Electronic Security Perimeter allows considerable flexibility for the entity to determine which security controls to apply, because of the significant number of Low Impact BES Cyber Systems.

Commenters suggested requiring a banner on Medium and Low Impact BES Cyber Systems. However, the SDT disagrees and felt the requirement to have "appropriate use banners" was administrative; therefore, it has been removed.

#	Organization	Yes or No	Question 34 Comment
34.1	CWLP Electric Transmission, Distribution and Operations Department	Agree	As long as TFEs are available for systems that do not support the password requirements.
34.2	Bonneville Power Administration	Agree	But see comments on R14.2, above. In addition, 14.4 is only acceptable if the definitions of remote access and external connectivity are changed, as discussed above. A banner is appropriate for someone accessing a BES Cyber System from completely outside the control of the entity.
34.3	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
34.4	FirstEnergy Corporation	Agree	With the exception of the concerns presented in the previous question.

#	Organization	Yes or No	Question 34 Comment
34.5	Oncor Electric Delivery LLC	Disagree	(R14.2)Multifactor authentication in legacy substation devices is extremely difficult and not needed. Appropriate logging and access controls will eliminate most threats. (R14.4)Appropriate Use Banners are not possible on many legacy dial-up devices used in substations. Appropriate logging and access control will eliminate most threats.
34.6	Southwest Power Pool Regional Entity	Disagree	14.2 and 14.4 should also apply to Medium impact BES Cyber Systems.
34.7	US Army Corps of Engineers, Omaha Distirc	Disagree	14.2 Multifactor authentication will be a major burden for small IT staffs. Standard should offer alternatives to mitigate - stronger passwords and or more frequent password changes.
34.8	WECC	Disagree	14.3 should be required for low impact.Remote access controls should apply to all impact levels.
34.9	Black Hills Corporation	Disagree	14.4 should be “Required” for all. Others are OK.
34.10	ERCOT ISO	Disagree	14.4: Should apply to Medium Impact BES Cyber System.
34.11	Tenaska	Disagree	18.1 all should be each.19.1 Validation of inbound data is more often done on the host application level and not at the boundary or host level.19.2 Is this RTU data? The protection is done at the applications level and I cannot examine data at my perimeter if it is encrypted at the host level.
34.12	Progress Energy (non-Nuclear)	Disagree	Believe it should be required for Low, Medium and High for R14.1, R14.2 and R14.2.
34.13	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
34.14	The Empire District	Disagree	Comments: We believe items 14.3 and 14.4 are going to set the stage for numerous

#	Organization	Yes or No	Question 34 Comment
	Electric Company		TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.15	E.ON U.S.	Disagree	E.ON U.S. believes that the proposed time requirements are not reasonable and require 24x7 support personnel with the privilege to revoke access.
34.16	Entergy	Disagree	Entergy believes some aspects of R11 and R14 are redundant and suggests combining them. We also believe criteria in R14 should apply to high, medium and low risk assets and provide a footnote indicating that where requirements are unable to be met explicitly that the strongest possible controls should be employed alternatively.
34.17	Dominion Resources Services, Inc.	Disagree	High Impact should be removed from 14.1 since it is covered by 14.2.
34.18	GE Energy	Disagree	If user accounts are audited on Medium Impact systems (see question 20), there should be an appropriate use banner.
34.19	LCEC	Disagree	Is this for remote access and wireless network access or does it also apply to wireless communications between BES Cyber System Components?
34.20	US Bureau of Reclamation	Disagree	It would seem that this criteria is in conflict with sound business practices. The concept of allowing access by default to Low Impact BES Cyber Systems does not make sense. Add deny access by default requirement for low systems. Specific access permissions are not required, however.
34.21	MidAmerican Energy Company	Disagree	Items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.Table R14 should be rewritten in a manner that minimizes TFEs. As an example, eliminate the word upon in 14.4 to eliminate TFE for systems that can only display banners immediately after access.

#	Organization	Yes or No	Question 34 Comment
34.22	National Grid	Disagree	National Grid suggests having 14.3 for Low Impact systems as well.
34.23	NextEra Energy Corporate Compliance	Disagree	NextEra believes Medium Impact BES Cyber Systems should have to comply with requirement 14.4. However, the rest of the impact levels are appropriate.
34.24	American Municipal Power	Disagree	Please provide a little or no impact category
34.25	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, and Table 14. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.
34.26	Garland Power and Light	Disagree	Requirement 14.3 and 14.4 Should add "required" to all impact levels
34.27	USACE HQ	Disagree	Requirements 14.3 should be required for every level of impact.
34.28	San Diego Gas and Electric Co.	Disagree	SDG&E believes that Medium impact assets should also be required to have multifactor authentication controls (within the definition question mentioned in Question 33).
34.29	ISO New England Inc	Disagree	Should apply to all
34.30	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in row 14.2.
34.31	Consultant	Disagree	Table R14 - Item 14.1 It seems illogical to require authentication controls on Low Impact systems when there is no Account Management required for these systems. Suggest deleting the requirement for Low Impact BES Cyber Systems.
34.32	Alberta Electric System Operator	Disagree	The AESO suggests adding the following to Table R14: o 14.3 - Required for Low Impact. o 14.4 - Required for Low and Medium Impact.

#	Organization	Yes or No	Question 34 Comment
34.33	Southern California Edison Company	Disagree	The same authentication methods should be applied to all Levels.Also, SCE requests that the drafting team provide justification for the lack of a deny access by default for low impact system.
34.34	Minnesota Power	Disagree	These impact levels are generally acceptable, however to maintain consistency with Table R10, Parts 10.4 and 10.5, the High Impact cell in Part 14.1 should be blank since it is addressed in Part 14.2.
34.35	American Transmission Company	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.36	Florida Municipal Power Agency	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.37	MRO's NERC Standards Review Subcommittee	Disagree	We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.
34.38	Hydro One	Disagree	We don't understand the emphasis on wireless communication and believe that in the present form, it would be very complex to implement. It's our opinion that the protection should remain the same regardless of the type of access point.
34.39	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R14:R14 Table 14.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR14 Table 14.2: Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR14 Table 14.3: (if this requirement is retained)Low Impact: N/AMedium Impact: N/AHigh Impact: RequiredR14 Table 14.4: (if this requirement is retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required

35. Requirements R15 to R19 of draft CIP-011-1 concern procedures for system security protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R15 to R19? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1 R15 through R19 have moved to CIP-007-5 R1 through R4.

For physical ports and services, several commenters expressed confusion around the term "externally accessible." The SDT agrees, and "externally accessible physical ports" was removed and substituted with physical ports used for "network connectivity, console commands, or removable media."

In addition, for physical ports and services, commenters expressed concern that physical port protection seems unnecessary, since overall physical security and personnel vetting is required, and many devices do not allow for configurable disabling of ports. The SDT agrees the objective of disabling unnecessary physical ports is primarily to prevent accidental propagation of malicious code. In response, the requirement was modified to "restrict" access. A description of acceptable forms of restriction is included in the measures; for example, these could be physically disabling the port or including signage about the use of ports.

For security event monitoring, several commenters stated that there is no need for weekly log review/clarity or manual log review since continuous monitoring is required. The SDT disagrees and references paragraph 528 of the FERC Order 706 that provides context for a weekly log review. The requirement allows for a review to include a sampling or summarization of security event logs.

For security event monitoring, several commenters expressed concern that there is no definition of "cyber security event" (i.e., a normal good logon is a "security event"). The SDT agrees and has modified the requirement to ensure that audit events must be organizationally defined. An enumerated list of events in the Standard is of little value.

For security event monitoring, commenters expressed concern that the requirement can be interpreted to include monitoring and logging for systems that don't support this functionality. The SDT agrees, and in response, this requirement was modified to apply log generation to the BES Cyber System (rather than the component) and allow the entity to define the generated events to audit.

For patch management, commenters expressed concern that not every patch is applicable to a BES Cyber System. The SDT agrees with this observation and notes that this requirement should be covered through the patch evaluation process. The focus of the requirement should be a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner."

For patch management, commenters expressed concern that flexibility is needed for the installation of patches; these dates can be based on equipment outage schedules, which could change the frequently or grid conditions that may or may not allow patching. The SDT agrees that the date of installation needs to be flexible to take into account equipment outage situations or high risk system conditions that could present an undesirable time for installing patches. Requiring an install date for the patches does nothing to improve BES Cyber System reliability. The overall goal of security patching should be to decrease the latency between security patch release date, application vendor certification date, entity testing, and implementation date. The SDT has revised the patch management requirements to achieve this goal.

For patch management, some commenters posed the question of what starts the clock for patching (release vs. availability vs. OS vendor vs. control system vendor). The SDT agrees there should be a starting point, but requiring an install date for the patches does nothing to improve BES Cyber System reliability. In response, the requirement has been modified so that Responsible Entities are required to create or revise an implementation plan within 30 days of the patch release from the identified source of the patches.

For malicious code prevention, commenters posed the question of whether the standard requires testing against actual malicious code. In response, the SDT disagrees and feels the intent was strictly focused on insuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.. This has been clarified in the guidance for the standards.

For malicious code prevention, commenters expressed there is still nothing specifying that malicious code prevention does not apply to field or network equipment. The SDT agrees, and in response, the requirement was modified to include malware prevention processes. It is now much more a “what” and not a “how” level of requirement.

#	Organization	Yes or No	Question 35 Comment
35.1	Dairyland Power Cooperative		15. It is good that this section is not wrongly specific as CIP-007:R4 is. This should allow for solutions that are not specifically signature based. This should allow for a network-based solution rather than individual solutions on each component. BES systems should not be used like typical Internet user systems, and therefore it should not be enforced that Internet user solutions be applied.16.2 requires a fixed implementation schedule of patches. However there should be an allowance that not every little security patch needs application, and it should be acceptable to defer insignificant patches until a later date when a significant patch needs to be applied. Additional controls to compensate may not be needed other than the security already designed to isolate a BES cyber system.17.1 Focusing on documenting the process to

#	Organization	Yes or No	Question 35 Comment
			harden seems wrong-the focus should be on requiring/verifying that a system is hardened. 19.1/19.2 How is validating inbound data (19.1) different than determining if inbound data has been compromised (19.2)? Was the intent of 19.1 to validate/authenticate the remote host/application on inbound connection? There should be requirements to restrict inbound connections from known remotes only. Validation of data should be defined. Perhaps inbound need definition too. Is it inbound initiated connection vs. data transferred inbound regardless of initiation direction?
35.2	National Rural Electric Cooperative Association (NRECA)		In R17.1, what specifically is the mitigation plan required to address/accomplish? Please ensure this requirement is clarified to explain this better.
35.3	Progress Energy (non-Nuclear)		R16.2 fixed dates for generating stations that depend on outages for implementing this is impractical as outage dates frequently change. Also, the ambiguity from v1-v3 (resulting in so many TFEs) remains here and still needs to be addressed.R17.2 - do not understand the externally accessible port requirement, there are no externally accessible physical ports outside of the six-walled boundaries, requirement not needed.CIP-011 R15 - Require detecting and responding to introduction of malicious for Medium Impact Cyber Systems which could be an electronic relay, what if there isn't a commercial solution for installing malware detection for relays or any other electronic device that runs with only proprietary closed firmware? Would it be impractical to require this only for devices that run a general purpose programmable commercially available operating system such as Microsoft Windows Operating System variants/UNIX and LINUX variants/SUN SOLARIS variants/Apple OS variants, etc --- or Is there going to be TFE process for these such as for switches, etc.?We like that this requirement does not require the use of traditional virus protection software.CIP-011 R18.3 - Requirement to keep logs of system events for 1 year for each high impact device could be massive in terms of storage and archive and may not be technically feasible for electronic relays.CIP-011 - R19 table - Need additional clarification as to what data validation methods (data integrity checking) are to be

#	Organization	Yes or No	Question 35 Comment
			employed. Can this be satisfied solely by employing Secure FTP or Secure ICCP for all inbound data?Calibration ports on programmable relays must remain open for calibration but this requirement would require rendering them unusable. We want to ensure this use is interpreted as “normal” operations.CIP-011-1 R15.3 (System Security) - The statement ‘Implement processes to test and update malicious code protections’ should be clarified to specify that in no case should malicious code be purposefully exposed to operational BES Cyber Systems as a part of this testing.CIP-011-1 R16.2 (Security Patch Management) - Requiring a ‘fixed date for either installation of the applicable patches or completion of mitigating measures that address the vulnerability’ is too inflexible in a real world where such activities may need to be accomplished during the next plant outage.CIP-011-1 R19 (Communications and Data Integrity) - This sounds like a ‘best practices’ type of requirement, but depending on how BES Cyber Systems are defined, this could require redesign/implementation of front-end processors on all inbound traffic to all Control Center BES Cyber Systems. Such a requirement cannot be quickly implemented without significant potential impact on the BES. We would like to suggest that this be listed as a requirement for any new BES Cyber System implemented at a Control Center.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security.”
35.4	FEUS	Agree	Agree with Comments: The drafting team should consider revising the wording of 17.1 from ‘implement a mitigation plan’ to ‘implement mitigating measures’ to reduce confusion with mitigation plans submitted to correct a violation.
35.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R15.This is very poorly worded, and too open to interpretation on a number of areas.15.1 - how do you audit this item? FMPA suggests: “Document and implement procedures implemented to limit the

#	Organization	Yes or No	Question 35 Comment
			propagation of malicious code."15.3 - This could be interpreted to read that you need a full-scale development environment/copy of your production system to introduce malware to and guage the responsiveness of the mitigation techniques you put in place. If the intent of the standards is to protect the BES, by testing malicious code on systems that's not helping anyone. Time should be spent making sure it doesn't happen, not testing to see what happens when you introduce it. FMPA suggests "Review logs of malware detection systems within the following time periods: 30 calendar days for medium impact, 7 calendar days for high impact."R16.FMPA agrees with the intent of this standard; however there are some underlying issues that should be addressed before the standard is implemented. One such example might be a requirement to change out hardware to meet a new patch released by a vendor; before equipment is purchased it has to be tested - in some cases equipment shortages may make it impossible to comply with the 30-day requirement.R17.17.1 - How does "external connectivity" apply to network ports being shut down? Does that mean for devices that route data to other external networks?17.2 - What does "externally accessible physical ports" mean? Does this refer to ports that are connected via Ethernet cable to an area outside of the protected area? If so, the standard should explicitly say this.R18.18.1 - Requiring components that do not have logging capabilities to be monitored could be a real problem. While there are a number of technical ways to accomplish logging of systems, there is no clarity in the standard as to what is and is not acceptable levels of logging on a device - this needs to be better defined. FMPA suggests "Implement automated tools or organizational processes to monitor and log all available system events that are related to cyber security for all BES Cyber System components." This would give more flexibility in collecting data from other centralized devices (such as SCADA systems) and limit the data collection to what is available.18.2 - what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining criteria?18.3 - what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining criteria?18.4- what is the definition of "Cyber Security"? How does one know what does or doesn't relate if there is no defining

#	Organization	Yes or No	Question 35 Comment
			criteria?R19.This is a very difficult implementation. As a general comment, if the intent is to protect the BES, perhaps more effort spent on ensuring that no unauthorized machine can communicate with BES components is a better place to spend effort.
35.6	Emerson Process Management	Agree	For R16, keeping cyber systems current so that they can be supported with security patches is very essential in maintaining system security. This should be a requirement under R16 and provide a TFE opportunity if this can not be met immediately, but with a auditable mediation plan.
35.7	SCE&G	Agree	How does the SDT intend to account for equipment incapable of supporting certain requirement (e.g. malicious code)? Will the TFE process be utilized. If so, it would be helpful for entities to see where the SDT envisions initially allowing for TFEs.
35.8	Southern California Edison Company	Agree	SCE requests guidance on whether the list of requirements apply to each component or if they only apply at a system level. For instance, can testing and malicious code protection in R15.3 be performed at a system level or should each component demonstrate this capability?A separate standard with highly prescriptive methods to document situations where it is not technically possible to implement a certain control, controlled and auditable documentation of mitigation plans will enable registered entities to record instances of non-conformity.A prime example would be that R 17.1 may be impossible to implement because of the technical design for a particular device. While the standard allows or a mitigation plan, the draft does not indicate whether or not the lack of such capability is a case of strict compliance.
35.9	Nebraska Public Power District	Agree	Security protection for cyber components that cannot connect to an external network do not require the same level of protection as those cyber components with connectivity to an external network. I recommend adding an exclusion to R16 and R18 for cyber components that cannot be connected to an external network.
35.10	USACE - Omaha Anchor	Agree	This is a less strenuous requirement than previous version of CIP. Previously every

#	Organization	Yes or No	Question 35 Comment
			item in the ESP had to comply - requirement states every system must comply - implying not every item must comply as long as the system does.
35.11	Xcel Energy	Agree	While we agree overall, we do have some suggestions/requests for clarification1. R15 to R19 should allow for TFEs2. R18.4/R20.6 We do not agree with a need to review logs every 7 days.3. R19.1 Further definition is needed of the expectation to "Validate data". Our concern is if were to include RTU data that can not be validated. A TFE allowance may be needed in this case.
35.12	Independent Electricity System Operator	Disagree	- R15.1 define malicious code. For R15 and sub requirements, does malicious code mean AV or Spyware detection/prevention or does Malicious code require a code review when deploying code and patches to systems?- - R16.2 does not require that the mitigatio
35.13	National Grid	Disagree	1. Inconsistency in using "processes" versus "one or more processes" in all requirements. National Grid suggests using "one or more processes". 2. Recommend new wording for 15.2 similar to 26.2 -Respond to the detection of malicious code.3. Recommend new wording for 15.3 - Implement processes to test and update protections in place to respond to the detection of malicious code.4. Recommend using the controls for Low Impact BES CS too since once the code is propagated it spreads across network irrespective of low/medium/high BES CS.5. Recommend changing 16.1 from "release" to "availability". 6. Recommend removing "with a fixed date" from 16.2 because the cyber system may not be available for maintenance due to grid system conditions.7. Request a R17 local definition of "attack surface".8. 17.2 - recommend changing "externally accessible physical ports" to "externally accessible physical communication ports". Also please clarify external to what.9. Request a local definition of "security events".10. In 18.2, is the SDT considering providing the timeline for issuing alerts and also to respond to those alerts? 11. Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.12. Recommend that 18.4 be re-worded to be consistent with FERC Order P526 - "Some manual review of logs to improve automated detection settings, even if

#	Organization	Yes or No	Question 35 Comment
			alerts are employed on the logs."13. Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven days.14. Recommend that R19 should "insure the integrity of the data."15. Recommend that 19.1 should be "Entity should document process to insure the integrity of the data link between the BES Cyber System and the remote node." This new 19.1 should be "Required" for High Impact and Medium Impact BES Cyber Systems.16. Recommend that 19.2 should be "Where links cannot be secured, the Entity shall document the mitigation in use." This new 19.2 should be "Required" for High Impact and Medium Impact BES Cyber Systems.
35.14	Southwest Power Pool Regional Entity	Disagree	15.1: The criteria should "limit the introduction and propagation of malicious code." 15.3 should require such testing prior to implementation rather than assuming. The objective statements in R16 and R18 are prescribing a requirement through the use of the statement "to ensure." 16.1: Clarify who is "releasing" the security patch. For example, is it being released by the operating system vendor (e.g., Microsoft) or the third-party application vendor (e.g., the EMS/SCADA vendor) subsequently certifying the patch against the supported application? 16.2: Clarify that compensating measures must be implemented within a prescribed timeframe after determining a security patch to be applicable unless the patch is installed within that prescribed timeframe. If compensating measures are implemented as an interim measure, they must remain in place until the security patch is installed with the understanding that the compensating measures can be improved during the interim period. 17.1: The term "mitigation plan" has an enforcement connotation. Consider requiring the documentation and implementation of compensating measures instead. 17 overall: there are a number of additional system hardening techniques other than disabling logical and physical ports. Additional hardening should be required for High impact systems. See the baseline configurations found on the Center for Internet Security web site for additional information. 18.2: This requirement presumes 100 percent availability of the monitoring process, which is unreasonable for automated solutions. Additionally, prescribe a timeframe for issuing alerts for detected system events.

#	Organization	Yes or No	Question 35 Comment
			18.3: Consider rewording the criteria to read “Maintain logs of system events related to cyber security for the specified time period.” 18.4: The requirement to maintain records documenting the review of logs is a compliance evidence issue and should not be included in the requirement. 19.1: Questionable if this is an auditable requirement. Clarify what is intended by inbound data validation? 19.2: Encrypted data does not mean uncompromised / valid data. Is this requirement essentially the same as 19.1? Is this asking for the validation process to be external to the normal validation processes included in the application software running on the BES Cyber System? Is this an indirect requirement to implement “Secure ICCP?”
35.15	Regulatory Compliance	Disagree	15.3 - STRIKE "testing" from the criteria. There is very little bennefit to test signature. 16.1a - Need clarification on components not patchable.16.b for those devices that are patchable - assessment of patches within 30 days.16.2 - Clarification - assess whwther vulnerabilities exist for a device.17.2 - need definition of external connectivity - more guidance on physical switch ports18.4 - propose 30 days for 30 days for manual review of automated systems - it is redundantR19 - wait and see - need guidance
35.16	LADWP	Disagree	15.3 states to test and update malicious code protections. Testing the code protections should be removed.
35.17	Network & Security Technologies Inc	Disagree	16.1 - Please clarify meaning of “release” of security patches by specifying patch source (the corporation, organization, or individual that wrote it?). This matters because some application vendors combine O/S patches in “bundles” they release to customers with service contracts.17.2 - Given the restrictions on physical access and the requirements to train and background check personnel with unescorted physical access to BES Cyber Systems, this requirement seems unnecessary. Moreover, on any given day it may be very difficult to predict whether a given physical port might be of use in an emergency troubleshooting or restoration situation. Could be contentious during audits.R18 - Does the SDT intend that Responsible Entities be able to, if necessary, determine what user(s) was on what system and when? If so, this

#	Organization	Yes or No	Question 35 Comment
			requirement should be made explicit.19.1 - Please clarify types of “inbound” data this requirement applies to. Operational data only? Mirrored backup data received at a backup Control Center from a primary Control Center? An emergency “hot fix” from a SCADA/EMS vendor? Meaning of “validate” also needs to be clarified. SDT has solicited input on which proposed requirements should be “eligible” for TFEs - surely this is one. Depending on the intent of this requirement, “data validation” may be something that can only be done in a useful/meaningful way by application logic.19.2 - We consider this to be an unenforceable requirement and therefore suggest it be dropped unless compelling evidence exists that replay and/or MITM attacks are a real and growing problem. Investigating a single occurrence of invalid data could consume scores of person-hours, lengthy interactions with communication providers, other Responsible Entities (e.g., for a BA that operates a Control Center that receives all its data feeds from other companies), and even law enforcement with no guarantee of success. Cryptographic protection of in-transit data, even if achievable (probably not unless a Responsible Entity owns and/or controls both ends of the data feed), offers no protection against corruption of data at the source and could also cause latency issues.
35.18	ERCOT ISO	Disagree	16.1: Clarify “release” from whom--the product vendor (e.g., Microsoft) or other vendor that prohibits installation of a patch until certified with their applications?17.1: Compensating measures should be allowed in instances where a mitigation plan to achieve strict compliance is not possible. 18.2: Specify the timing for responding to alerts. 18.3: Should be removed to data retention section. 18.4: Should address the use of automated security event monitoring systems. TFEs should be allowed for R16. TFEs should be allowed for R17.TFEs should be allowed for R18.TFEs should be allowed for R19.
35.19	MidAmerican Energy Company	Disagree	16.2 - Define when the implementation schedule needs to be completed by and define how far in the future the installation can be scheduled. For example a patch is assessed within 30 days; the currently wording would allow me to develop an implementation schedule a year later and the schedule could call for the installation

#	Organization	Yes or No	Question 35 Comment
			to take place three years later. 17.2 Change to “Disable, render unusable or configure such that it has no access to a BES System” This would allow us to put ports into logical VLANS that do not have access to the BES Systems.19.1 What does “validate data” mean? This sounds like in would need to be an application level control. Is that what is intended?
35.20	PacifiCorp	Disagree	16.2 - Define when the implementation schedule needs to be completed by and define how far in the future the installation can be scheduled. For example a patch is assessed within 30 days; the currently wording would allow me to develop an implementation schedule a year later and the schedule could call for the installation to take place three years later. 17.2 Change to “Disable, render unusable or configure such that it has no access to a BES System” This would allow us to put ports into logical VLANS that do not have access to the BES Systems.19.1 What does “validate data” mean? This sounds like in would need to be an application level control. Is that what is intended?
35.21	ReliabilityFirst Staff	Disagree	16.2 - need a time frame (60 days), for row 17.1 does there need to be a time frame for implementation of a mitigation plan?
35.22	Luminant	Disagree	17.1 implement a mitigation plan or compensitory measures
35.23	Progress Energy - Nuclear Generation	Disagree	Agree with Table 15, R16.2, Table 17, 18.1 AND 18.2. R15-R19 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments. Durations for R16.1, R18.3, and R18.4 should align with comments in Attachment 1.
35.24	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.15.3 should include more clarification on what "testing" entails and whether that just refers to signature updates.Recommend replacement of the word "known" with "discovered" in R18. 18.4: more clarity

#	Organization	Yes or No	Question 35 Comment
			needed regarding the allowance of both automated and manual review of logs. R19 creates a potentially impossible level of obligation. Recommend striking.
35.25	American Transmission Company	Disagree	As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.26	MRO's NERC Standards Review Subcommittee	Disagree	As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.27	Western Area Power Administration	Disagree	Assuming one can detect and respond to the introduction of malicious code, how is it expected that we limit propagation of malicious code? By definition, malicious code is often not detected, and if it is detected (by virus prevention software, for instance), that software generally quarantines or deleted the malicious code automatically. This section seems to need a little thought as to what is really being required. This opens up technical interpretation of what "limits" malcode. This also assumes only a specific

#	Organization	Yes or No	Question 35 Comment
			vector (rootkit, malware, virus/worm) but doesn't address Denial of Service attacks which could be much more serious. Maybe they need to specify intent. R16: A plan for every patch as opposed to relying on the change control process? This seems excessive.R17: Seems to be an improvement. For 17.2, does this mean plug up physical ports like USB? This is unclear. If it does, cannot rely on physical perimeter for protection?R19: Since this applies only to external connectivity (ICCP connections or equivalent), how is it intended that we validate the actual data coming into the system? What level of validation? Ex: end-point validation (ipsec and certs) vs application endpoint (ssl), the way this is worded it goes WAY beyond this. This is not a communications validation issue. Are they wanting to get to MITM attacks? If so it isn't clear.
35.28	E.ON U.S.	Disagree	CIP-011, R15.1 Limiting propagation of malicious code is an integral part of any standard A/V protection. If this requirement is calling for something more than this then the requirement should be clarified to remove this ambiguity. If it is one and the same as R15.2, then E ON U.S. suggests combining these two sub-requirements.CIP-011, R17.2 The term "...externally accessible physical ports" is ambiguous. Does this refer any externally-facing port through which a party may attempt to gain unauthorized electronic access to a BES Cyber System Component? Or, does this refer to an externally-facing port directly on the BES CSC itself?CIP-011, R18.3 The requirement to maintain logs for one year is a significant burden. This can be a tremendous amount of data depending on the level of logging enabled.CIP-011, R18.4The expectations regarding review of logs should be more clearly defined. The whole point in having "continuous security monitoring for detected system events" is to avoid the extremely burdensome requirement of manually sifting through tremendous volumes of log data. Though some mechanism should be in place to ensure the automated logging and alert systems are not disabled, the requirement to manually review system logs is excessive and provides little if any security enhancement.CIP-011, R19.1The expectations for validation of data inbound to a BES Cyber System should be more clearly defined. How is this reasonable to be accomplished? Parameter checking is already a common mechanism within most

#	Organization	Yes or No	Question 35 Comment
			SCADA / DCS systems, but this does not protect against tampering or data manipulation within the prescribed bounds for a given data point.CIP-011, R19.2 Same comment as for R19.1...how is this to be accomplished?
35.29	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
35.30	The Empire District Electric Company	Disagree	Comments: As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.
35.31	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy has the following concerns with requirements R15 - R19:R15 - A TFE may be required for programmable electronic devices within a substation environment where is not technically feasible to manage malicious code.R16.1 - The definition of a “release” needs to allow for vendor verification of the applicability of a patch to a given systems functionality before the thirty day clock begins.R17.2 - CenterPoint Energy recommends clarification as to what are considered "externally accessible physical ports" R18 - the phrase "related to cyber security" is ambiguous. R18.2 -implementing "continuous security monitoring that issue alerts for detected system events related to cyber security" would seem to require installation of external communications to remote substations increasing their vulnerability. R18.4 - A manual review every 7 calendar days is overly burdensome. Automated processes are already mandated to detect and alert personnel of cyber security events. CenterPoint Energy recommends a 30 day review.R19.1 - Concerned

#	Organization	Yes or No	Question 35 Comment
			with the method to "validate data inbound to a BES Cyber System". This requirement is intended to address data integrity issues associated with man-in-the-middle attacks, but it does not specifically address the issue. It leaves open the issue of data which was intentionally or unintentionally manipulated by responsible entities. The issue becomes something different if our Control Center must validate data from a Reliability Coordinator or Transmission Operator which has been intentionally or unintentionally modified by trusted personnel. Data integrity implies encryption. This requirement should state: “One or more of the following encryption standards are required to ensure data integrity inbound to the Control Center.R19.2 - Concerned with ability to provide evidence that we "evaluate invalid data inbound to a BES Cyber System" to determine whether the data has been compromised maliciously with current systems capability. As stated previously, this requirement does not address the issue of malicious entities entering malicious data from the endpoints. This requirement is an attempt to address issues associated with MITM attacks. Inherent in the various SCADA protocols is error detection and data delivery, but not data integrity. The ICCP protocol is encapsulated within TCP/IP. The TCP/IP protocol will ensure communication reliability and error detection, but it will not ensure data integrity.
35.32	Entergy	Disagree	Entergy suggests making requirements in general apply to high, medium, and low assets alike and provide a footnote to allow a TFE for assets which are not capable of meeting the requirements. 17.1 suggests that unused network ports only have to be disabled in the event there is external connectivity. This requirement appears to be extremely relaxed from version 1. The current language suggests that the perimeter firewall can be used to control port usage thus relieving the requirement to control at the asset itself. In 17.2 there is a reference to externally accessible physical network ports. Entergy suggests language change to just say “unused physical network ports.” In 18.2 there is a time requirement of maintaining logs for 1 year for high and 90 days for medium. Maintaining logs for 1 year can be problematic due to the amount of space required. Suggest making requirement for 90 days for high, medium and adding the same requirement for low assets. Also suggest adding a footnote to allow TFE for

#	Organization	Yes or No	Question 35 Comment
			assets that are unable to meet requirements. In R19 it appears the requirement is to encrypt all data coming into a BES Cyber System. The intent is to ensure data integrity. Most EMS systems have CRC checks, and reasonability checks, etc., embedded in the systems to validate the integrity of the data being received. Entergy does not believe that encryption is required for all digital data as it greatly increases overhead, operation and troubleshooting of the data networks. Entergy suggests that encryption should be required for remote access as remote access connectivity many times traverses the Internet or some non-private network links at some point. Entergy suggests providing alternate methods to validate inbound data rather than encryption.
35.33	Southern Company	Disagree	For 17.2, what does this mean? An externally accessible physical port would require a switch next to an open window or something.R15.3 requires testing of malicious code protections. This is an effort better left for malware protection suppliers. Often only the production system is available to the end user, the quantity and frequency of malware release prohibit an effective end user test program.R16.1 requires assessment of security patches within 30 days of release. This assessment is typically performed by control system supplier to assure that no adverse impact occurs to their product. Often only the production system is available to the end user. The end user has no control over vendor testing schedules. If this requirement is placed on the end user MS KB977165 type “blue screen” events may occur.R16.2 The requirement of a fixed date for patch installation may not be possible in all cases if a system restart is required for an operating unit.For R15 & R16, there is the potential that implementing malicious code detection and security patch management on substation devices could interfere with the primary function of these substation devices which is the reliable delivery of power.For R17.2, what will be considered acceptable for rendering physical ports unusable? We should not be required to permanently disable ports thereby making the ports unavailable for future use.For R18, not all BES Cyber System components in substations are capable of monitoring and logging system events.For R18, implementing security monitoring processes on substation devices may interfere with the primary function of these substations devices which is the reliable delivery of

#	Organization	Yes or No	Question 35 Comment
			power.R18.2 Clarify intention, is continuous monitoring with manual review of logged alerts acceptable? What is a "detected system event"? Is a single or double incorrect password attempt an alarmed event?R18.1 requires an automated log system R18.4 requires a review of log events. Is a manual review of all logs required in an automated system or just the alarms?
35.34	Detroit Edison	Disagree	In 15.2, "respond" is vague. Propose rephrase to read "Detect the introduction and mitigate the effects of malicious code."Remove table entry 19.1 since it is redundant to 19.2.The term "applicability" in 16.1 is vague. Consider introducing vulnerability severity classifications to patch management that determines the action and timetable required. Please note that this is submitted for consideration as a concept. The language and time tables will need further review and editing before this would be ready to add to the standard. o Level 4 - Intruders can easily gain control of a BES Cyber System Component, which can lead to the compromise of BES Cyber System security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the introduction of backdoors. High: patch within 7 days; Medium: patch within 14 days; Low: patch within 30 days. o Level 3 - Intruders can possibly gain control of a BES Cyber System Component, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. High: patch within 14 days; Medium: patch within 30 days; Low: patch within 90 days. o Level 2 - Intruders may be able to gain access to specific information stored on a BES Cyber System Component, including security settings. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files, directory browsing, disclosure of filtering rules and security mechanisms, and unauthorized use of services. High: patch within 30 days; Medium: patch within 60 days; Low: patch during next system maintenance window. o Level 1 - Intruders may be able to collect sensitive information from a BES Cyber System Component, such as the precise version of software installed, open ports, services, etc. High: during next system maintenance window; Medium: during next

#	Organization	Yes or No	Question 35 Comment
			system maintenance window; Low: Patch during next system maintenance window.
35.35	RRI Energy	Disagree	In regards to 17.1, for clarification purposes, based on the definition of external connectivity written in the Standard, if a web server is actively listened on port 80 inside the BES boundary protection but is not accessible externally from the outside of the BES boundary protection, the Responsible Entity does not have to report and assess that port and service.In R17.2, what does externally accessible mean? Ex. Physical port is on a device that is in a cabinet, the cabinet is within a building, and the building is within a fence-lined property. Is the port non-accessible? What type of physical ports are we trying to protect? Is it only physical "network" ports? How about USB ports, PC (PCMCIA) Card slots, CD/DVD drives?Not all devices can be logged such as PLC's, meters, etc.; therefore 18.1 should allow for a TFE.In regards to R19, what defines an internal versus external boundary. Within a single facility, are all boundaries internal? If cables transverse hallways between "computer rooms" within a Control Center does an external connection exist? Can a back-up control center be an extension of a primary control center where all data connections between the control centers are considered "internal"?
35.36	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
35.37	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R16, but recommends changes as follows: o Regarding Part 16.2, this requirement contains no timeframe by which this schedule must be developed. If it was intended that the development of this schedule is to coincide with the activity described in Part 16.1, then that should be explicitly stated. Also, there is no limitation regarding how far in the future is reasonable to set the "fixed date." Minnesota Power recommends that if a timeframe for the "fixed date" is not established in the Standard then there should be a stipulation that if the date for installation of the patch is greater than a pre-determined amount (say 45 days), then mitigating measures need to be in place until the security patch is implemented.Minnesota Power generally agrees with the

#	Organization	Yes or No	Question 35 Comment
			proposed Requirements R17, but recommends changes as follows: o Regarding Part 17.1, the first sentence creates some confusion. Minnesota Power recommends that it be reworded as follows: “One or more processes to ensure that for each BES Cyber System Component, only those network accessible ports and services that are required for normal and emergency operations are enabled.” o For Part 17.2, is it the Standards Drafting Teams intent that a CD or DVD drive be considered an “externally accessible physical port?” If so, this should be explicitly defined. Logically, mounting a DVD is no different than plugging a memory stick into a USB port.Minnesota Power generally agrees with the proposed Requirements R18, but recommends changes as follows: o If it is the Standards Drafting Teams intent that Requirement R18 apply only to cyber security events, then Minnesota Power recommends that the term “security events,” which is used throughout this requirement, is reworded to state “cyber security events.” o Regarding Part 18.1, the Standards Drafting Team should consider clarifying the timeframe within which the monitoring of system events should occur (i.e., real-time, minutes, hours, days, etc.). If monitoring is done using a manual process, rather than an automated tool, real-time may not be possible, and guidelines should be established regarding how quickly events must be examined. o Is it the Standards Drafting Teams intent that Part 18.1 address the collection of security events into logs and Part 18.2 address the process to review and act upon the logs collected under Part 18.1? If so, the Standards Drafting Team should consider wording that would clarify the differences between these two Parts. o In Part 18.2, does the term “continuous” refer to “real-time?” If so, Minnesota Power recommends changing the term to real-time to avoid confusion. o Minnesota Power recommends rewording Part 18.3 as follows: "Retain logs of system events related to cyber security for the specified time period." o Minnesota Power recommends communicating all time frames in calendar days to eliminate confusion regarding what constitutes “1 year.” o Regarding Part 18.4, if 18.2 provides for “continuous” monitoring of system events for these same systems, why is it also required that a Registered Entity manually review these logs? In addition, can the Standards Drafting Team provide guidance regarding what should be included in this review? On an SEIM, for instance,

#	Organization	Yes or No	Question 35 Comment
			these logs can be enormous - to the point that manual review is not possible within reasonable time constraints.Minnesota Power generally agrees with the proposed Requirements R19, but recommends changes as follows: o Regarding Part 19.1, How, in real-time operation, can external data be validated (protocols already validate message structure)? For example, an LBA receives unit set-points from its ISO-BA via ICCP. If the data being received is within operating limits for that unit, it is "valid." The ISO may truly be requesting the unit to drop by xx MW. How is that differentiated from someone altering an inbound message to maliciously tell a unit to drop by the same xx MW value? The process for echoing values back to the external system does not solve this, since this, too, can be manipulated. o Part 19.2 appears to be a specific instance of Part 19.1 and given that this Part starts with the phrase "Where not cryptographically protected," it seems that Part 19.1 may be misstated. Is Part 19.1 supposed to discuss "protecting" inbound data, rather than "validating" it, via encryption, authentication, etc.? Also, in Part 19.2, what constitutes "invalid" data? Is this data which is outside of normal operating limits? Or maybe outside of reasonability limits? Again, maliciously inserting perfectly normal or valid data could have detrimental effects to the BES, whereas "invalid data" should, by default, be thrown out by normal processing.
35.38	Idaho Power Company	Disagree	Need to put a limit on how far out the fixed date should occur for implementation or mitigation of security patches. R18 refers to security events but the sub-requirements refer to system events related to cyber security. Need to make this clearer that the focus is on abnormal system events as a normal authorized log-in is a normal security event but not one that needs review or response.
35.39	NextEra Energy Corporate Compliance	Disagree	NextEra believes the current language did not provide clear guidance and is too lax which leaves room for interpretation. The following are the recommended updates for the requirements:15.1 - Implement technical, procedural and/or process controls to limit the impact of code which modifies or destroys data, steal data, allow unauthorized access Exploits or damage a system, and does something that user did not intend to do. o Implement technical controls, where technically feasible, to

#	Organization	Yes or No	Question 35 Comment
			detect and mitigate malicious code o Implement technical and/or procedural controls to limit the propagation of malicious code o Implement technical and/or process and procedural controls to respond to introduction of malicious code15.2 - Malicious code protections should be updated at least on a quarterly basis if applicable updates are available and technically feasible. Updates should be tested prior to implementation to ensure no adverse impact by the software updates.As far as the order of requirements, detection should come first and it should be a requirement by itself. Combined 15.1 and 15.2 and removed 15.3 from the initial version.NextEra believes the implementation of processes incorporating the criteria specified in CIP-011-1 Table R16 - Security Patch Management in order to ensure that security vulnerabilities in BES Cyber Systems are mitigated was not clearly identifiedThe current language did not provide clear guidance and left room for interpretation. The following are the recommended updates for the requirement: 16.1 - The Responsible Entity shall establish a security patch management assessment program to track, evaluate, and test cyber security patches within 30 calendar days of their release to validate their applicability to its BES Cyber Systems.16.2 - The Responsible Entity shall develop an implementation schedule with a fixed date for either installation of the applicable security patches or the completion of mitigating measures that address the vulnerability if application of the security patch is not technically feasible.It should be stated that there needs to be a program to track, evaluate, and test cyber security patches within the defined timeframe that are applicable to the BES Cyber System.It is also recommended that there is more in depth guidance on the implementation schedule.CIP-011-1/R17Did not account for technical feasibility for disabling of ports.The following are the recommended updates to the requirements:17.1 - Implementation of process (es) to ensure that only those network accessible ports and services required for normal and emergency operations are enabled. In cases where unused network accessible ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document and implement compensating measures to mitigate the risk of exposure.If it is not technically feasible, the entity must have documented compensating measures to mitigate the

#	Organization	Yes or No	Question 35 Comment
			risk of exposure. This requirement should be applied to Medium and High BES Cyber Systems.The CIP CIP-011-1 Table R18 - Security Event Monitoring to ensure that security events are known, logged, and responded to on BES Cyber Systems did not provide enough guidance.The current language did not provide clear guidance and left room for interpretation. The following are the recommended updates: 18.1 - Implement automated tools or organizational processes to monitor and log system events that are related to cyber security for all BES Cyber System components, where technical feasible. Instances, that are not technical feasible the Responsible Entity shall implement manual processes to mitigate risk exposure.18.2 - Implement and document security processes for continuous (24/7 365 days, except when conducting system maintenance of the monitoring devices) security monitoring that issue alerts for detected system events related to cyber security.18.3 - Maintain system logs of system events where technical feasible, related to cyber security within the specified time period. If not technically feasible, the Responsible Entity shall document and implement manual processes to mitigate risk exposure.18.4 - The Responsible Entity shall verify that the log and alerting system is working in the time intervals mentioned. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs within 90 daysAdded language provides more definition.The CIP-011-1 Table R19 - Communications and Data Integrity to protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems did not provide enough guidance.The current language did not provide clear guidance and left room for interpretation. The following are the recommended updates:19.1 - Validate data inbound in the Control Center for specific connections and verify if those are the correct connections. 19.2 - Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to the BES Cyber System in a Control center to determine whether the data has been compromised. All unauthorized access attempts to a control center must be identified and investigated.Added language provides more definition.Also, In 15.1, please clarify the term "limit propagation". How would a Responsibility Entitity demonstrate the compliance to 15.1? Is a documented

#	Organization	Yes or No	Question 35 Comment
			technical or procedural control to limit the propagartion of malicious code sufficient? Furthermore, NextEra asks that examples be provided on how to meet this requirement at BES Transmission Facilities where all BES Cyber System Components are not capable of running anti-virus software.In 16.1, is the assessment necessary when regular patch cycle or planned installation is under 30 calendar days?In 16.2, what is a reasonable "implementation schedule with a fixed date for either installation of the applicable security patches or completion of mitigating measures that address the vulnerability"In 16.2, is an implementation schedule necessary when regular patch cycle or planned installation is under 30 calendar days?In 16.2, if the "installation of the applicable security patches" would cause a risk on the availability and performance of BES Cyber System, is it sufficient to complete the mitigation measures that address the vulnerability? If so, we propose that the language of 16.2 be modified to have this as an option in lieu of the installation of the applicable security patchesIn 17.1, does this apply only to BES Cyber System Components that are accessible from the outside? If yes, does this apply only to the ports that are externally connected or for all ports if the BES Cyber system Component has external connectivity?In 18.4, please clarify the term "review logs of system events" -- how will compliance be demonstrated?In 19.1, how do we validate data inbound to a BES Cyber System in a Control Center? Please provide methods that could be employed by the Responsible Entity. Could 19.1 and 19.2 be simplifeid by jjust requiring cryptographic protection for High Impact BES Cyber System in a Control Center?Regarding R-18, the log review of assets is too short. (i.e. 30 / 7 days). With this constraint, there will be limited knowledgeable personnel available for review. Some systems do not provide data to allow for this type of analysis. Need support from external vendors, which may not be feasible on a weekly / monthly basis. Due to volume in the industry, it is anticipated that vendor resources will be limited to support us in this capacity. NextEra suggests at least quarterly for Medium / High.18.1 states logging events "related to cyber security". This is subject to broad interpretation and should be clarified. NextEra suggest providing specific examples, such as: Abnormal System Shutdown Account Lockouts Admin User Account Changes

#	Organization	Yes or No	Question 35 Comment
			All Domain Account Logon Failures All Group Account Changes All User Account Changes All Policy Changes Domain Admin Acct Logon Failures Domain Admins-Admin Group Acct ChgDomain Admins-Admin Group ChgDomain Trust Rel Policy ChangesEvent Log FullLogon Logoff SummaryNormal System Startup-ShutdownPassword Changes and ResetsSecurity Log ResetsSrv Wkst All Logon FailuresTerm Srv All Logon Logoff SuccessesTerm Srv All Session Discon-ReconUser Account Creation or DeletionUser Account Password ChangesUser Rights Policy Changes18.2 uses the term "issue alerts" which could imply alarming or otherwise performing a notification. If NextEra had to raise an alert for every system event we could potentially have a continuous alarm stream. If it is determined that event alarms are necessary, then the events have to be further defined and our systems have to be specifically tuned on site for the real running environment.NextEra recommends defining the term further to either include explicit alarm/notification or not. Would also push further for alert in the form of logging to be reviewed or alarmed for review.19.1 states validate data inbound to a control center. Data should be further classified as data directly related to real-time BES operation. If a Monitoring and Diagnostics Center is classified a control center they would potentially have to perform data validation on all historical data made available to that center, depending on interpretation. An alternative is to further classify or define "validate" to allow validation simply by verification of traffic from a reliable source, i.e. identifying the source historical data server.NextEra proposes considering validation of the originating source rather than validating the data itself.
35.40	Con Edison of New York	Disagree	o R16.2 requires a “fixed date” for apply security patches or mitigation. This requirement does not take into consideration that entities may require vendors to test the patches on their systems before they will be applied to operational systems. The release dates for these patches is not fixed by the vendor. The requirement should allow for the planned install date to be a fixed period after the patch is tested and available to the user. A fixed date may be a challenge when predicated on manufacturer certification which may introduce unnecessary risks to operations. o R17.1 “external connectivity” is expected to mean external to the (ESP) boundary. o

#	Organization	Yes or No	Question 35 Comment
			R17.2 It is not clear what externally accessible physical ports includes. External to the location or external to the device (i.e.: located on the front of the workstations) o R18.2 - need clarification on type of events that need continuous monitoring; security logs can be voluminous with excessive informational notifications o R18.4 - if automated tools are used this should not be required o R19 - need more info on ensuring data integrity. What does "external" mean? Does this require special checks of RTU inbound data? Unclear what will be considered validation. Is Encryption validation? If the RTU data is not encrypted is the EMS validation of data sufficient? If the systems (especially legacy equipment) do not support integrity checks the addition or development may not be possible or recommended. Will this require a TFE?
35.41	Puget Sound Energy	Disagree	Puget Sound Energy has the following comments:R15.1 - Puget Sound Energy feels that "Limit propagation..." is an abstract term and needs clarity to it in order for NERC to be able to consistently validate compliance.R15.3 - Puget Sound Energy suggests clarity to what type of testing is required of malicious code protections. Is NERC requiring functional testing that the malicious code protections are reliably functioning or security testing (penetration testing)?R17.1 - Puget Sound Energy would like clarity into the degree of documentation required to validate compliance with "...required for normal and emergency operations are enabled." Puget Sound Energy would also like clarity into NERC's definition of "enabled" and "disabled". For example, can network accessible ports be "enabled" and "disabled" through the use of host based firewalls?R17.2 - Puget Sound Energy suggests that the disabling of physical ports on BES Cyber System Components only be required where physical security protections are not required, as outlined in Table 5. If physical security is provided, per Table 5, then the disabling of physical ports seems unnecessarily redundant. Puget Sound Energy would like clarity on "externally accessible physical ports", in cases where the BES Cyber System Component is physically protected by measures outlined in Table 5.Table 18 - Puget Sound Energy suggests including "Where Technically Feasible" to R18, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 18. For example, entities may incorporate

#	Organization	Yes or No	Question 35 Comment
			dialup accessible devices that, by the nature of a connection that is built up and torn down as necessary, is incapable of providing “continuous security monitoring that issues alerts”.R19.1 - Puget Sound Energy requests clarity into what NERC means by “validate data inbound”. “Validate” is subjective and Puget Sound Energy would like clarity on how entities can prove compliance. Puget Sound Energy would also like clarity into the scope of the inbound data it must validate. For example, is NERC asking for validation of interconnections with other utilities and balancing authorities or validation of every RTU that provides an inbound data stream to a control center’s BES Cyber System?
35.42	BCTC	Disagree	R15 - Â Change title to “Prevent Malicious Code”Â 15.1 - suggest replacing the words “Limit propagation” to “Prevention”Â 15.3 - we do not agree with this requirement. Recommend removal of the words “to test”. It is not a good practice to introduce malicious code into a BES Cyber System - even in QA!Â Another potential area for TFEsR16 - Â R 16.2: if the patch results in a system upgrade it could take up to 6 months to implement the patches; if the patch does not result is a system upgrade then recommend allowing 30 days to implement said patchesR17 - Â The requirements needs to provide more guidance on how to provide evidence for open/ closed TCP (static) versus UDP (dynamic) ports Â R 17.1 Guideline would be appreciated on how to meet this requirement. We have struggled with this one in the past.Â Provide a definition of what is “system hardening” R 17.2 - what is the objective of this requirement? We feel that simply disabling a physical report does not provide much value from a security perspective (i.e. can unplug an active port and plug in an unapproved device); instead we recommend locking down devices’ MAC addresses as this would result in a more secure environmentR18 - Â R18.3. A year seems excessive to require an entity to retain ALL logs. What is the objective in requiring utilities to do this?R18.4. Suggest breaking this one in to two requirements - one for log review and the other for maintaining records - current wording can be interpreted as having to retain events for medium impact systems for a longer period than high impact? R19 - Â R19.1. We request a definition of what is meant by “validation” as well as guidance on how to perform this taskÂ Potential area for TFEsÂ

#	Organization	Yes or No	Question 35 Comment
			R19.2. We are struggling with how to comply with this requirement. We have an IDS implemented in our environment where users are alerted on suspect packets - is this what this is referring to? Intent not clear with the current wording.
35.43	WECC	Disagree	R15 - alright with all criteria, R16 - alright with all criteria, R17 - Item 17.1 should cover local ports and services not just network ports and services. Consider removing the words "network accessible" like text in previous standards and make required for Medium and High impact levels. Physical ports should be rendered unavailable on components of Medium impact systems as well as High. Item 18.2 needs to define "continuous" or remove it from the criteria. R17 - Consider adding more criteria for system hardening including system base-lining or move system base-lining from the change management section to here. Look for other overlap between R17 and change management. R19 - agree with criteria but would suggest adding the following after validate data "(eg. syntax checking, bounds checking, sanity checking, etc)"There needs to be more language specifying a definition of malicious code, what it means to limit its propagation, and to detect and respond to its introduction. As written, there is very little to audit against in this requirement.Additional language is needed to describe what it means for a patch to be released.System hardening should be required for all systems, not just those that are externally connected.Additional language is needed to clarify the requirements for security event monitoring, for example, what continuous monitoring means.Log review intervals are too long to be effective.The data integrity criteria are good additions but need additional language to clarify the intent. What does it mean to validate inbound data? Also, consideration should be given to the fact that cryptographic protection is not fully effective in all circumstances. More direction is needed as to when cryptography is an acceptable control. Also there are no requirements in the standard that define criteria for cryptographic controls.
35.44	Alberta Electric System Operator	Disagree	R15 - Change requirement to include confidentiality, to address potential MITM or MITB attacks. "...malicious software that could affect availability, integrity, or confidentiality of the..."Table R16 - include additional row similar to 16.1, but to

#	Organization	Yes or No	Question 35 Comment
			assess security patches within 60 days. Make this a requirement for Low Impact BES Cyber Systems. All BES Cyber Systems should be assessed, however High and Medium Impact systems should be assessed sooner.Table R19 - 19.1 states "Validate data inbound to a BES Cyber System in a Control Center." And the corresponding impact states "Required for external connectivity only." Based on the definitions, "inbound to a BES Cyber System" can only be from a device "external to the BES Cyber System" so the impact is redundant. Similar situation for 19.2. Suggest changing "Required for external connectivity only" to "Required". Table R19 - consider adding additional rows to Table R19 to address validating inbound data to BES Cyber Systems that are not in a control centre. 19.1 Validate data inbound to a BES Cyber System in a Control Center. Required for Medium and High 19.2 Validate data inbound to a BES Cyber System. Required for High19.3 Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to a BES Cyber System in a Control Center to determine whether the data has been compromised maliciously. Required for Medium and High19.4 Where not cryptographically protected, develop and implement a process to evaluate invalid data inbound to a BES Cyber System to determine whether the data has been compromised maliciously. Required for High.
35.45	LCEC	Disagree	R15 - Testing for malicious code protection is not auditable.R16 - Device end of life support issues need to be addressed. Release needs to be clarified to address the situation where a vendor may release a security patch for a BES Cyber System Component but it is not yet approved by the BES Cyber System vendor.R17 - o It is not often clear whether the standard is referring to logical and physical ports. Physical, logical or both should be specified any time the term port is used.R18 - What constitutes a security event?Is the 90 day requirement meant to be an absolute 90 days as opposed to 3 years and 90 days to be able to show compliance?R19 - How would one validate inbound data? Was this clearly meant to be data integrity as opposed to data protection? Why was this scope chosen?
35.46	Dominion Resources	Disagree	R15 - The stated intentions of the SDT at the May Workshop were to reduce TFEs and to distinguish between Control Centers vs. Substations and Power Stations. Neither

#	Organization	Yes or No	Question 35 Comment
	Services, Inc.		of these stated goals is presented in R15. TFEs will be required for 15.2 and 15.3 and there is nothing indicating that these should not apply to field equipment or network equipment (e.g., firewalls, routers, switches). Dominion agrees with the stated intentions of the SDT team.To avoid the potential for TFE's associated with R15.2 and R15.3, a footnote similar to the one used for Table R10 on Page 11 of CIP-011 should be added. Also, access controls related to access points would be better addressed in the Boundary Controls Section of CIP-011.R16.2. The word "fixed" should be replaced with "planned" to allow some flexibility for installing the patch. 17.2. It should be clarified that an alternative where the equipment does not provide a configurable method of disabling the port is that methods, such as using security tape, to indicate any tampering with the port may be used.18.2. This section will require a TFE since many devices do not have the capability of issuing alerts. A footnote to avoid need for a TFE should be added.18.3. One year is too long to maintain logs for network devices. Storage space is at a premium. There will be a substantial increase in cost to increase storage space for each high impact cyber system This should be changed back to 90 days for High Impact cyber systems. 18.4. Logs of system events should only be required to be reviewed every 90 days. Logs should be reviewed only when an alert is issued for a detected system event. Routine reviews would take an extraordinary amount of time with no expected substantial results. R19. Common methods for ensuring data integrity include physical protection of the asset, authentication and authorization of data sources/inputs, using data validation and error checking rules at the application or database level, and a variety of other technical, operational and management controls. Dominion recommends the wording used in R19.1 be modified as follows to state the objective without specifying how it should be accomplished since the methods vary depending on the nature of the system and the technology in use:"19.1 Implement methods to maintain the integrity of data inputs to a BES Cyber System in a Control Center. " 19.2. It is sometimes impossible to determine if data has been compromised. Dominion understands that the proposed re-wording for 19.1 will also suffice to meet the requirements for 19.2 and recommends that 19.2 be removed.

#	Organization	Yes or No	Question 35 Comment
35.47	FirstEnergy Corporation	Disagree	R15 - We prefer the new text over the old CIP standards and it would reduce TFEs. In R15/Table 15: need some type of exception for devices incapable of running anti-malware.R16 - We prefer the new text over the old CIP standards. R17 - We prefer the new text over the old CIP standards.R17/Table 17: Need clarity on "externally accessible and physical ports". Does that mean serial, parallel, USB, Fireware, etc. or ports that are capable of transmitting routable protocols (e.g. network interface cards).R18 - 18.4 - Need greater clarity around whether automated alarming can be used rather than manual review of system event logs. Also - should it be specified somewhere in R18 that these sub-requirements apply to electronic security only, not physical security events (which is spelled out in R6)? 18.2 - We question the use of the word 'continuous' in this sub-requirement as this would be difficult for those entities that use 'organizational processes' to monitor and log.R19 - Overall this requirement appears to be too broadly worded. 19.1 - The use of the word 'validate' seems vague. Is the intent of the SDT that entities provide the specifics on what 'validate' means - e.g. the appropriate data or a point-for-point comparison, how often, etc? 19.2 - Many existing systems do not provide a means to accomplish compliance with this sub-requirement - for example, legacy RTU protocols. R19/Table 19: Need clarity on "invalid data". How do you evaluate invalid data?
35.48	US Army Corps of Engineers, Omaha Distirc	Disagree	R15 needs to be limited to general processing equipment. Requirement for anti-virus type software on all systems will numerous TFE's. R18 logging of all BES Cyber System components will generate numerous TFE's. R19 concerned about what realistic measures are available to meet requirements.
35.49	US Bureau of Reclamation	Disagree	R15.3 - If it is truly intended that entities test malicious code protections (not just ensure signatures are up to date and that protection software is running, the Standard should provide some additional guidance. Few entities are going to be willing to introduce malicious code, even into a test system, to verify malicuious code protection. Further, there is not timeline for when the malicious code protection must be tested. It would not be unreasonable to require and annual test of the

#	Organization	Yes or No	Question 35 Comment
			malicous code protections. The malicious code protections should be an intelligent requirement. Some devices that are not addressable may not need malicious code protection. R16.2 - Suggest the phrase "if the patch will not be installed" be added to the end of the requirement. R17.2 - Is locking within an enclosure satifactory? R18.3 - Suggest medium impact requirement be "for at least 90 calendar days" and that high impact timeframe be considered for reduction, perhaps to at least 180 calendar days.R19.1 - Explain how this is to be accomplished within the Standard - based on some specific criteria. This requirement is too open-ended. Since the concept of BES Cyber Systems now includes such devices as programmable multifunction or solid state relays, the requirement to "validate data" inbound makes no sense. Many of these devices reside within a control center. The definition now includes those center which are used to control more than one BES generator. The data going into the relays is from transducers either inside or outside the physical security perimeter but within another physical security perimeter. This data may be digital or analog. How would it be validated, cryptographically progracted or analyzed for malicious compromise?It is not clear how an "interactive user" session would apply to "programmable" relays.
35.50	Ameren	Disagree	R16.1 - This requirement should address documenting the installation date of patches and that patches have been installed.R18 - should only apply to network based systems with external connections only; currently this required is not limited on what it applies to.R19.1 and R19.2 - There is no way to comply with this standard without requiring the vendors to write better code. Suggest removing these requirements.
35.51	Northeast Utilities	Disagree	R17 appears to be significantly weaker than the previous standards. It also does not appear to align with the draft change control standards. Ports and services are a strong control to ensure only services required for operation are allowed. At minimum the High Impact BES Cyber systems should be “Required”.R19 needs more explanation. What does validate data mean?

#	Organization	Yes or No	Question 35 Comment
35.52	Hydro One	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious code.Requirement 15.3 implies that testing ensures that the deployment will not adversely impact security. However, the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing 16.1 from “release” to “availability”.Recommend removing “with a fixed date” from 16.2. The cyber system may not be available for maintenance due to grid system conditions.Request a R17 local definition of “attack surface”.Recommend changing 17.2 from “Disable, or render unusable, externally accessible physical ports” to “Disable or secure externally accessible physical communications ports”.Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.Requirement 18.4 seems to have one purpose and that is to prove 18.2. To us this seems redundant since R18.2 require alert for system events. Why do we need a review at some later point? We recommend removing the requirements R18.4 Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommend that R19 should “ensure the integrity of the data”.Recommend that 19.1 should read “Entity should document process to ensure the integrity of the data link between the BES Cyber System and the remote node.” This new 19.1 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should read “Where links cannot be secured, the Entity shall document the mitigation in use.” This new 19.2 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Please clarify the applicability of R19. Does this requirement apply only to code releases into the system or it applies only to external data streams (e.g. weather data from a service provider, data from RTUs etc)?
35.53	ISO New England Inc	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious codeBelieve the SDT meant that 15.3 testing insures that the deployment will not adversely impact security. However the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing

#	Organization	Yes or No	Question 35 Comment
			16.1 from “release” to “availability”Recommend removing “with a fixed date” from 16.2 because the cyber system may not be available for maintenance due to grid system conditions, implement based on your documented patch process. Request a R17 local definition of “attack surface”Recommend changing 17.2 from <<Disable, or render unusable, externally accessible physical ports>> to <<Disable or secure externally accessible physical communications ports>>Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber SystemsR18.3 Some automated tools do not have separate log retention based on the asset. The log retention applies to all assets. It is unclear if the log retention is the actual log from each Cyber System component or the log that an automated tool keeps (ie parsed out info from syslog). Either way a years worth of logs will require terrabytes upon terrabytes of storage for useless information. Recommend that 18.4 be re-worded to be consistent with FERC Order P526 - <<Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs. >>Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven daysRecommend that R19 should “insure the integrity of the data.”Recommend that 19.1 should be “Entity should document process to insure the integrity of the data link between the BES Cyber System and the remote node.” This new 19.1 should be “Required” for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should be “Where links cannot be secured, the Entity shall document the mitigation in use.” This new 19.2 should be “Required” for High Impact and Medium Impact BES Cyber Systems.
35.54	Northeast Power Coordinating Council	Disagree	Recommend new wording for 15.2 - Respond to the detection of malicious code.Requirement 15.3 implies that testing ensures that the deployment will not adversely impact security. However, the existing words could be interpreted as testing the malicious code prevention by introducing malicious code.Recommend changing 16.1 from “release” to “availability”.Recommend removing “with a fixed date” from 16.2. The cyber system may not be available for maintenance due to grid system conditions.Request a R17 local definition of “attack surface”.Recommend changing

#	Organization	Yes or No	Question 35 Comment
			17.2 from "Disable, or render unusable, externally accessible physical ports" to "Disable or secure externally accessible physical communications ports".Recommend 18.3 should be 90 calendar days for High Impact and Medium Impact BES Cyber Systems.Recommend that 18.4 be re-worded to be consistent with FERC Order 706 paragraph 526 - "Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs."Recommend that 18.4 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommend that R19 should "ensure the integrity of the data".Recommend that 19.1 should read "Entity should document process to ensure the integrity of the data link between the BES Cyber System and the remote node." This new 19.1 should be "Required" for High Impact and Medium Impact BES Cyber Systems.Recommend that 19.2 should read "Where links cannot be secured, the Entity shall document the mitigation in use." This new 19.2 should be "Required" for High Impact and Medium Impact BES Cyber Systems.
35.55	USACE HQ	Disagree	Requirement 15.1 should be deleted from the list. Limiting the propagation of malicious code is a logical step in the "respond to the introduction of malicious code" phase, process which is required in 15.2. Therefore 15.1 present a possible double jeopardy since it is logical to think that when responding to the introduction of malicious code in the environment the steps will include limiting the propagation of the same before removing it from the system. Also, requirement 15.1 language is to broad in the interpretation of it. "Limit propagation of malicious code" implies that the code has moved through some part of the system, therefore the question is, how much movement of the code is acceptable when creating a response process?. The acceptable answer to this question could depend on the auditor's subjective views of what is acceptable safe propagation of the code inside the system.
35.56	Garland Power and Light	Disagree	Requirement 16.1 - Reword requirement to say assess within 60 days - reason is because we feel it is adequate to check the vendor web site every 30 days and allow 30 days for testing and determination of implementationRequirement 18 - Reword

#	Organization	Yes or No	Question 35 Comment
			requirement to allow for Responsible Entity to develop a definition of a "system security event". The words are used in the main requirement and each subrequirement. Requirement 19 - o Delete Requirement R19 - Control systems currently validates data for quality and limits and then tags the data with any issues so that downstream applications can handle appropriately. This is sufficient for the security and reliability of the BES. R19 is impractical for implementation in the field for large or small utilities. This will reduce reliability of the overall system.
35.57	Oncor Electric Delivery LLC	Disagree	Requirements 15.1 and 15.3 are not necessary. The use of antivirus and malware software is problematic on some systems, while “whitelisting” requires additional hardware which may contain its own vulnerabilities. Detection and response should be sufficient. Many programmable devices are not capable of propagating malicious code or running prevention software.Requirement 18.2 does not apply to many legacy cyber systems and should only be applicable to systems which utilize routable communications.
35.58	Manitoba Hydro	Disagree	Revise the wording of Requirement R15 to “... integrity of the BES Cyber Systems.” Please clarify the intent of “test and update malicious code protections”. Requirement R16.2 should be revised to indicate the development AND implementation of the schedule. The wording of Requirement 16.2 currently does not require the application of mitigating measures prior to the installation of the applicable patch, and may need to be revised. For Requirement R17, please what is the meaning of “network accessible ports”, and “externally accessible physical ports”. Are physical ports enclosed within an unlocked cabinet “externally accessible ports”? Are physical ports within a non-public space, “externally accessible ports”? Requirement R18 does not contain any requirement for response to security event alerts or monitoring. Remove the word “maliciously from Requirement R19.2. It may be very difficult to determine if the data compromise was malicious or not. There are no specifics given with respect to “limit” propagation in Requirement R15.1. It is assumed to be at the Responsible Entity’s discretion in terms of criteria, means, etc. There are no specifics given with respect to “validate” data in Requirement R19.1 so it is assumed to be at the

#	Organization	Yes or No	Question 35 Comment
			Responsible Entity's discretion in terms of criteria, means, etc.
35.59	San Diego Gas and Electric Co.	Disagree	SDG&E thinks that R17.2 sounds good in theory (disabling external physical ports on assets), but in practice this can be difficult to achieve without damaging the port for future legitimate use. Many shops use epoxy or other glue-based products to physically disable / protect such ports, and these solutions tend to be permanent. If we are physically protecting the asset from access anyway with card readers and other physical means, why is it necessary to take this redundant step of sealing physical ports on assets when only people with authorized physical access (who have had training) can actually access the asset?SDG&E has concerns about the viability of complying with R19.1 (validating inbound data to a BES Cyber System in a control center) in a situation where the incoming data is encrypted. How does the SDT define "validate"? Where does the validation need to occur?SDG&E also has concerns about the viability of complying with R19.2 (evaluate invalid data for malicious compromise) without MUCH additional vendor support. How does the SDT define "evaluate invalid data"?
35.60	Platte River Power Authority	Disagree	Suggested Revision (clarify what to test):15.3 Implement processes to update malicious code protections including testing security controls
35.61	Duke Energy	Disagree	Table 15: will need a TFEWithin generation, we have differing opinions on the definition of code. Suggest clarifying that it does not include programming code.Requirement 16.1: Assessment of security patches within 30 calendar days of their release for applicability to its BES Cyber Systems. Release from whom? It makes a big difference if the patch is released from Microsoft, for example, or the patch is released from the control system vendor (e.g. Emerson, Invensys, Areva, etc.) as to how/if the patch is implemented to prevent risk to the BES cyber system.Table 17: for devices inside a locked cabinet, are the physical ports on that device externally accessible?Requirement 17.2: how does the definition of "externally" in "externally accessible physical ports" compare with the definition of external in "external connectivity" in R3? Also, this definition implies that there are physical ports that are

#	Organization	Yes or No	Question 35 Comment
			NOT “externally accessible”. Need to make definition more clear. Suggest taking out reference to “externally accessible”.Table 18: 18.1 - not all devices are capable of logging, need a TFE18.2 - it would be helpful to have a definition of ‘events related to cyber security’18.4 - remove for systems where automated tools are in place. Requirement 18.2: " one or more security processes for continuous security monitoring" - is there any interpretation of the expectation here so that we don't have disagreement at audit? Are alternate controls allowed for BES Cyber Components that don't support logging/monitoring (example: manual review of physical access logs for stand-alone equipment)?Table19:Item 19.1 & 19.2 Additional explanation is needed to explain acceptable threshold for “validation of inbound data.”Clarify validate in 19.1. Is encryption a form of validation?What is meant by Data in 19.1?Requirement 19.1: What types of data validation controls are acceptable to meet this requirement? For example, control totals, presence check etc. Requirement 19.2: Need to provide an example with what methods can invalid data be evaluated to conclude that the data has been compromised maliciously?
35.62	Consultant	Disagree	Table R15 - Item 15.3 The requirement to "Implement processes to test and update malicious code protections." is confusing. Is the intent to "test malicious code protections and update malicious code protections" or to "test updates to malicious code protections" Please clarify the intent. There is a need to distinguish between updates to the malicious code protection "software" and malicious code protection "signature files". The software should be implemented in accordance with change control processes. The "signature files" are a specific subset of update to malicious code protection where it is unlikely a registered entity would have the capability to test what are typically vendor proprietary file formats. The extent of the 'testing' necessary for these signature files should be clarified.Table R16 - Item 16.2 While the concept of a "fixed date" sounds good, the requirement should allow for reasonable scheduling, including rescheduling, of the installation of applicable security patches or completion of mitigating measures. An option could be to remove the words "with a fixed date" and add a new item that would require that "Events that delay a security patch implementation schedule greater than thirty days shall be documented."Table

#	Organization	Yes or No	Question 35 Comment
			R17 Item 17.1 The first sentence uses the terminology "network accessible ports and services" and the second sentence uses the terminology "network accessible services and communication methods". Suggest using consistent terminology to avoid confusion.Suggest defining the term "network accessible ports and services" (may be multiple terms) as they are intended for use in the standards. There does not appear to be a standardized definition for this term in the industry. The term "network accessible ports and services" appears to imply access across the protection boundary? If it does then the requirement statement of "Required for external connectivity only" is unnecessary and should be changed to "Required".Table R18 - Item 18.3 Suggest changing the word "within" to the word "for" for clarity of meaning.Item 18.4 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 18.1 and 18.2 require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Table R19 - The limitation of these items to a Control Center is an added dimension of Impact that is not included in the impact categorization criteria. If data is an issue, then these requirement should apply to all assets based on impact categorization without addendum or modification by the requirement. Suggest modifying the impact categorization criteria to clearly identify those assets.Table R19 - "Inbound data" implies remote access, and the terminology "Required for external connectivity only" is redundant. Suggest changing the wording to "Required".Items 19.1 and 19.2 are inconsistent. Item 19.1 requires validation of inbound data, and item 19.2 provides an exception to validation for encrypted data. If you comply with item 19.1, then item 19.2 is irrelevant. If you comply with item 19.2, then you are in violation of item 19.1.R19 - Overall, this requirement should be removed in it's current form. Automatic system operation cannot exist if "inbound data" is required to be validated. Automatic system operation is dependent on responses to external data inputs. If the intent is to return the BES to manual operation, this requirement

#	Organization	Yes or No	Question 35 Comment
			will achieve that end.
35.63	American Electric Power	Disagree	Table R15: 15.1, regarding "Limit propagation of malicious code", suggest replacing "propagation of" with "propagation and introduction of".15.2, regarding "Detect and respond to the introduction of malicious code." Would this be covered in a traditional cyber security incident response program? This should already be covered in R27.Table R16:16.1: Regarding the word "release" within "Assessment of security patches within 30 calendar days of their release for applicability to its BES Cyber Systems." Release from who? For example, is it the release of a new patch by Microsoft, or is it the certification of the patch by the control system vendor that the patch does not negatively impact the control system? Further clarification is needed. Patches released by Microsoft are not typically tested for several days or weeks by Control System vendors to validate that the patch does not impact functionality. Industry cannot test software patches as thoroughly as the Control System vendors.16.2: Is it a violation if you do not meet the fixed date? Suggested wording: replace "fixed date" with "scheduled date". Add a provision to supply reasoning for not meeting scheduled dates. The rewording provides flexibility to the Responsible Entity to push installation of the patch to a later date without being in violation.17.2: Add a sentence similar to the last sentence in 17.1, "In the case where unused, externally accessible physical ports cannot be disabled, the Responsible Entity shall document and implement a mitigation plan." The disabling of physical ports is not supported by all network devices. To meet the literal wording an entity may need to physically damage equipment which would void warranties and prevent further vendor support.18.1: Regarding "organizational processes" and "system events that are related to cyber security". Is it reasonable to think this can be done without automated tools?18.2: Regarding "continuous security monitoring", is this redundant to 18.1? If you are implementing automated tools to monitor and log system events are you not providing continuous security monitoring? Suggest removing these words to eliminate double jeopardy.This requirement should be focused on issuing an alert.Regarding "system events related to cyber security", what constitutes a system event related to cyber security? What criteria should be used? Is there an accepted

#	Organization	Yes or No	Question 35 Comment
			standard that an entity will be held to in an audit? If the right system events are not classified in an auditors' eyes, is this a violation? Suggest rewording to reference an acceptable set of minimal system events to monitor. What if a BES Cyber System does not generate a sufficient amount of detail to determine if a cyber security event occurred? Suggest allowing a TFE in this instance.18.3: Regarding "Maintain logs of system events related to cyber security within the specified time period", what if a BES Cyber System cannot store events for the duration required? Is a responsible entity required to go out to a device repeatedly to export their logs if they cannot meet the 90 day or 1 year increment? Suggest rewording to take into account limitations of BES Cyber Systems. Possibly use as a TFE item, if TFE's are maintained.What benefit does this provide for reliability or security? 18.4 is the important element, not the data retention.R19: With real-time or near real-time control systems, these requirements could increase latency and pose a negative impact to reliability.19.1: Regarding "Validate data inbound to a BES Cyber System in a Control Center", validate against what? Is the source being validated? Is the data itself being validated? Is providing encryption on the data sufficient? Who determines the appropriate level of validation? Is it being left to an auditor?Reliability could be compromised if this induces extra latency on the systems sending and receiving real-time data. This should be included as a TFE; older systems may not be able to handle the latency.19.2: Would "bad quality" indicators in the EMS system be an example of this?
35.64	APPA Task Force	Disagree	The APPA Task Force believes that Requirement R15 as currently drafted will require numerous TFE's. Each entity will need to document that they are not following this requirement since a vast array of devices in substations and generation stations are BES Cyber System Components but are not capable of propagating malicious code. Therefore we recommend the following edits for R15:R15. Objective:To protect BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions.R15. Requirement:Each Responsible Entity shall document and implement one or more processes incorporating the criteria specified in CIP-011-1 Table R15 - Malicious Code Protection. This requirement applies only to BES Cyber

#	Organization	Yes or No	Question 35 Comment
			System Components that have the capability to propagate malicious code. Change the Table legend to "Malicous Code Protections".The APPA Task Force is concerned that the criteria in R15 Table 15.3 do not constitute a reasonable requirement when looking at the transmission and generation environments that will be required to comply. The drafting team may not fully appreciate the full magnitude and implications of the phrase "test and update". We recommend that the criteria in Table 15.3 be removed or only be required for control centers.R16 Objective:To ensure that security vulnerabilities in BES Cyber Systems are mitigated. R16. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R16 - Security Patch Management R17. Objective:To reduce the available attack surface of the BES Cyber System.R17. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R17 - System Hardening The APPA Task Force agrees with the MRO-NSRS proposal noting that as written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings. This would require an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We recommend that this item be deleted.R18. Objective:To ensure that security events are known, logged, and responded to on BES Cyber Systems.R18. Requirement:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring R19. Objective:To protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems.R19. Requirement:Each Responsible Entity shall implement processes incorporating the criteria specified in CIP-011-1 Table R19 - Communications and Data Integrity The APPA Task Force is extremely concerned with the actual ability of the industry to comply with the criteria in R19 as proposed. A discussion is necessary to understand if this requirement is actually feasible for all entities with High Impact facilities.

#	Organization	Yes or No	Question 35 Comment
			Utilities hire capable operators to make decisions on incomplete data all the time. If validating the data inbound means another electronic verification, this is impractical. If validating the data inbound means calling a lineworker in the field to check a setting in a substation when an operator is not comfortable with the data he is receiving, this is reasonable, but still not an auditable requirement. We agree with the MRO-NSRS evaluation of 19.2, which notes that as written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously. We recommend that this requirement be removed and placed in the guidance in support of the standard as a future technology.
35.65	Bonneville Power Administration	Disagree	The objectives of these requirements ("to protect its BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions," "to ensure that security vulnerabilities in BES Cyber Systems are mitigated," "to reduce the available attack surface of the BES Cyber System, "to ensure that security events are known, logged, and responded to on BES Cyber Systems," and "to protect the real-time operation of the BES from the use of maliciously modified data by BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirements rather than appearing at the end of the requirements (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.The phrase "Reliability Functions" at the end of R15 is not a defined term in the April 20, 2010, Glossary of Terms Used in NERC Reliability Standards. Does the drafting team mean CIP-01-01 - Attachment 1, Functions Essential to Reliable Operation of the Bulk Electric System? If so, that should clearly be stated. If not, there should be a definition in the Glossary. Table 16, Section 16.2. We applaud the new standard, which makes it clear that immediate mitigation or installation of patches is not required. However, there are still some issues:1. Security patches arrive weekly to daily to multiple times a day. Many may be applicable to systems, but of minimal

#	Organization	Yes or No	Question 35 Comment
			threat. Entities should be able to not only evaluation the applicability, but the threat and risk of the threat to their systems within their environment, and choose to escalate or deescalate patches as appropriate to them. Low impact, or low risk patches may be assigned to a regular patch or maintenance cycle, while high risk patches may be tested and implemented immediately. This should be up to the system owners, and not prescribed in the requirement.2. Mitigation plans are not necessarily applicable. Some patches, while technically applicable to specific equipment or operating systems, may have such a low risk or impact that they entity may choose not to apply the patch.3. There are instances where a patch may be applicable from a security perspective, but the risk it presents from a reliability perspective may outweigh it. 4. Where systems are isolated from external affects, even a patch that applies to a specific device may not be necessary.5. Meaning of "fixed date" is not clear. Does it mean "the same for every patch", or "the date can't be changed"? Both are bad choices. Different patches might require different schedules, depending on their impact and the availability of outage time on the system.R17: Rename this back to "Ports and Services" to avoid confusion. In the electrical industry "Hardened" systems are those that meet specific electrical requirements and interference requirements.Also, the use of the word surface implies something physical rather than electronic.Recommendation for R17: "Objective 17 - To reduce the available electronic attack points of the BES Cyber System.R17. Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R17 - Ports and Services"Table 17, Section 17.1. A mitigation plan might not be appropriate. In the context of NERC standards, a mitigation plan describes the actions that will be taken to achieve compliance. That is not the situation here. Recommendation: "cannot be disabled, the Responsible Entity shall document the reasons for the inability and compensating measures used."Section 17.2. We understand that FERC wishes the standard to address physical ports. However, this could have negative conquences:1. There are hundreds of thousands of devices in service that have physical ports that may not be used. The fact that they are not needed or used normally means that there is nothing connected

#	Organization	Yes or No	Question 35 Comment
			to them. If there is nothing connected to them, they are not vulnerable to any kind of external or remote attack.2 - Disabling physical ports on electrical system components may be: o Impossible o Degrade the operation of the equipment o Render the warranties on the equipment void thereby removing vendor service o Create such a huge national work load that it could never be accomplished.Recommended change - Eliminate 17.2Table R18:18.1 & 18.2 - The use of the term "all BES Cyber System Components" is not accomplishable:1. Many, if not most "components" in the field do not capture what would be considered cyber security related events. They only capture electrical system events. They don't even have the capability to capture access events.It is the access points to these devices that may have the ability to capture even the most rudimentary cyber security information (Access Attempt, Date, Time, Account, Source, Target)2. It may not be possible to place monitoring equipment within electronic monitoring proximity of these components. 3. The term "events that are cyber security related" is not defined. What exactly does it mean? Is this access events, Intrusion Detection systems, Antivirus, ??? Much of this cannot be implemented on or even for "all BES Cyber Components". Recommendation: 1. Remove "components", so that the requirement is at the BES Cyber System level.2. Change "...security for all..." to "...security, as defined by the Responsible Entity, for all..."18.3 has the same issue with the definition of "events related to cyber security". In addition, this time frame has caused some confusion from an audit perspective. - Some have read that to mean that there must be, on the originating system, at all times, at least 90 days worth of logs. While others (rightfully, we feel) are maintaining archives of their logs in alternate locations for 90 days or longer. Recommendation: replace with "Maintain captured log information within the specified time period on-line, in archives, or in some other readily accessible form."Section 18.4. Consistently accomplishing manual review of logs could be difficult for large entities with large numbers of devices, especially within the 7 days required for high impact systems. The obvious solution is the use of an automated log review tool. This should be explicitly addressed in the standard. Recommendation: "Review, either manually or by automated means, logs...." Entries in Table R19 are acceptable only if the

#	Organization	Yes or No	Question 35 Comment
			definition of external connectivity is changed, as discussed above. Otherwise, entities would be forced to validate data inbound from one BES Cyber System to another BES Cyber System, all within the same Control Center. This does not seem to be the intent: using the existing definition of external connectivity, any data inbound to a BES Cyber System uses external connectivity. In that case, why state it so? Clearly, the intent was to validate traffic inbound from outside the Control Center, at most.
35.66	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The requirements are to prescriptive for the range of systems that it will apply to.
35.67	Constellation Power Source Generation	Disagree	The term “release” in R16.1 needs to be further defined. The issue with it being vague is that some patches for a system may be released for all users, but if that system is tied to a distributed control system, the distributed control system vendor has to validate the patch before its implemented by a facility. Using this example, there are really 2 release dates. For auditing purposes, a suggestion would be to define release locally as “the date of which a security patch has been safely validated by a vendor. If another vendor must validate this release before implementation, than the date it has been released by the second vendor will be used as the release date.” R16.2 is not worded correctly. A suggested change would be “Development of an implementation schedule with a fixed date for installation of the applicable security patches and a fixed date for completion of mitigating measures that address the vulnerability, until implementation of the patch.” In R18.1, is the monitoring and logging continuous, or on a fixed schedule? The SDT should add clarity to this requirement. R18.2 discusses issuing alerts but does not give a timeframe for issuing them. A suggestion would be 90 days to ensure a proper review of an incident to determine if it was a cyber event. At the CIP V4 Workshop, the drafting team stated that R18.4 was not meant to be an exhaustive manual review of logs, but rather a check to ensure the automated log is functioning. This needs to be included in the verbiage of the requirement. R19.1 should be reworded to say “Implement a process to validate data received by a

#	Organization	Yes or No	Question 35 Comment
			Control Center's BES Cyber System." Doing so would clarify R19 as a whole, and R19.2 can be removed due to its redundancy with R19.1.
35.68	Public Service Enterprise Group companies	Disagree	There are several clarifications necessary to make the language understandable and ensure that entities know what is required. [1] Please clarify the distinction between requirements 15.1 and 15.2. Performance degradations and potentials for false positives from detection mechanisms that inspect each file when accessed, as possibly implied by 15.2, may not appropriate for real-time systems. [2] In requirement 18.2 please specify what is meant by "continuous"? Is a periodic check sufficient? [3] Please clarify the distinction between requirements 19.1 and 19.2. In requirement 19.1 please specify what is meant by "Validate"?
35.69	Constellation Energy Commodities Group Inc.	Disagree	There is no definition of malicious code provided. Clarify the scope of malicious code to include virus, malware and spyware protection, as currently generally commercially understood.Please define the stipulation 'Required for external connectivity only'.Are the tools and processes listed in R18 intended to provide automated detection, or manual\narrative logging of events detected under the heading of other controls? If automatic, what sorts of events are contemplated? What is intended by the term 'Validate' in 19.1? Does this mean the identification of a separate, independent source for the data, business rules, or something else? Without understanding the intent of the standards drafting team, I cannot suggest specific changes.
35.70	Allegheny Energy Supply	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of

#	Organization	Yes or No	Question 35 Comment
			the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.71	Allegheny Power	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.72	EEI	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. Requirement 15.3 is unclear as to what is

#	Organization	Yes or No	Question 35 Comment
			meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.73	Reliability & Compliance Group	Disagree	To help eliminate TFE's here, you need to add a qualifier such as "to protect its BES Cyber Systems from malicious software that could affect availability or integrity of the Reliability Functions if mechanisms exist that can protect the BES Cyber System Component."
35.74	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
35.75	We Energies	Disagree	We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. If the purpose of this requirement is to limit the potential for automated propagation of malicious software, the requirement should be more specific and state that. The security problem of automated propagation of malicious software is different than the issue of change management and change control to verify that only authorized software is used. With respect to requirement 15.1, We Energies believes this may not be possible for non-windows based devices/systems.We Energies agrees with EEI: Requirement 15.3 is unclear as to what is meant by "Implement processes to test and update malicious code protections." Suggest "Implement processes to detect malicious software, and review annually".It may be appropriate to add language that is more precise regarding the attributes of the BES cyber systems/BES cyber components to be

#	Organization	Yes or No	Question 35 Comment
			protected. Is it sufficient for a relay (which has very limited operating system capability) to validate the specific version of firmware operating on it? It may be appropriate to add discrete requirements for systems that support the addition of anti-virus software. These requirements could require a validation of signature file updates prior to use on a production BES system. We Energies agrees with EEI: Specify in Table 19 that the requirements for Communications and Data Integrity apply to only to Control Centers.
35.76	GTC & GSOC	Disagree	We Recommend: 1. In R15.3: taking out the words "test and" or, alternatively, clarifying what is meant by "test"2. In R19.1: clarifying whether encryption is required or if CRC will be sufficient3. Completely removing R19.2 because of the following reasons referenced from the DHS Catalog of Control System Security: a. The use of cryptography within a control system will introduce latency to control system communication. The latency introduced from the use of cryptographic mechanisms must not degrade the operational performance of the control system or impact personnel safety. b. Failure of a cryptographic mechanism must not create a denial of service. Control systems generally support the objectives of availability, integrity, and confidentiality. Therefore, the use of cryptography should be determined after careful consideration.
35.77	Midwest ISO	Disagree	What does it mean to validate data in R19.1. What is the expectation if a piece of data has been changed/modified when the value received is within reasonable limits but is not the actual value sent? This could be particularly troubling for the Interregional Security Network and ICCP. For example, how can an RC validate that the SCADA system sent valid data to the ICCP server at a TOP if it is within an expected range? More details around the expectation of validating data would be helpful to ensure entities can be compliant.

36. Tables R15 to R19 provide direction concerning what impact level of BES Cyber Systems to which Requirements R15 to R16 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note: CIP-011-1 Requirements R15 through R19 have moved to CIP-007-5 Requirements R1 through R4.

Many commenters disagreed with the proposed BES Cyber System impact levels and made suggestions for improving these requirements, including suggestions to revise or refine the impact levels based on the particular characteristics of the BES Cyber Systems involved. For example, some suggested that certain requirements should apply only to Medium Impact BES Cyber Systems with external connectivity. Others suggested that there were key requirements such as malware prevention that should apply at all BES Cyber System impact levels. In response, the SDT has made changes to include an applicability column in each table for each requirement. The applicability column further refines the set of BES Cyber Systems and assets to which each part of the requirement must be applied. The intent of this approach is to refine, as commenters suggested, the scope of requirements that apply to each type of BES Cyber System or device based on its characteristics. The drafting team recommends that commenters carefully review the proposed applicability column in the table for each requirement in CIP-003-5 through CIP-011-1.

#	Organization	Yes or No	Question 36 Comment
36.1	Northeast Utilities	Agree	Need TFE language added; not all CCAs or protecting assets require malicious code protection.
36.2	FirstEnergy Corporation	Agree	R17 - Does ‘external connectivity only’ mean only firewalls? If not, please provide intent of SDT.
36.3	BGE	Disagree	15.1, 15.2 and 15.3 should also apply to Low impacted systems. 16.2 implies that the patching can only occur on the same day every month.19.1 Define “validate”.
36.4	ERCOT ISO	Disagree	15.1-15.3: Should apply to Low Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
36.5	American Electric Power	Disagree	17.1: Regarding "Required for external connectivity only" within the High and Medium

#	Organization	Yes or No	Question 36 Comment
			impact categories. Is this required for "routable external connectivity" only, or all connectivity?How will items in R18 and R19 be performed on systems with nonroutable connectivity? Will dedicated IT Security Operation staff need to be added to isolated networks to perform the security status monitoring?
36.6	US Bureau of Reclamation	Disagree	Add R15.1, R15.2 and either R18.1 or R18.2 to the requirements for a low impact system. Concept of REMOTE connectivity is not defined. Without that definition, it is hard to assess if a High Impact is appropriate or if no Medium Impact is reasonable..
36.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
36.8	Black Hills Corporation	Disagree	At least 15.2 and 16.1 should also apply to low impact BES Cyber Systems.
36.9	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
36.10	The Empire District Electric Company	Disagree	Comments: For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: “Required for routable external connectivity only”. We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.We believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally.
36.11	US Army Corps of Engineers, Omaha Distirc	Disagree	define terms "continuious security monitoring" and "detected system events."
36.12	CWLP Electric Transmission, Distribution and	Disagree	Due to the requirement for continuous monitoring and alerts defined in R18.2 the requirement for log reviews every 7 days should not be needed. A standard 30 day review as in the medium impact area should be appropriate for both high and

#	Organization	Yes or No	Question 36 Comment
	Operations Department		medium impact levels.Does the fact that the data has been successfully passed through a Firewall or Access List meet the obligation to validate data incoming to a Control Center in R19 or does this require the data be inspected all the way down to the packet level?
36.13	American Transmission Company	Disagree	For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.
36.14	MRO's NERC Standards Review Subcommittee	Disagree	For items 15.1 - 15.3, 16.1 - 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.We believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally.
36.15	Southern California Edison Company	Disagree	In order to appreciate the impact based categorization and reflect the actual impact on BES reliability, an additional requirement can be added to R16 for medium and low impact system. The drafting team should look at NERC PRC standards on maintenance schedules and synchronize CIP patching and upgrades to a maintenance and inspection schedule that is already mandated by NERC.Requirement R18 requiring logs be reviewed manually every seven days, when controls to automatically monitor such logs are already in place, is a control that does not seem to add additional security value. If the intent of the drafting team is to manually ensure and certify that the logging capability is functioning adequately, the drafting should include such verbiage. The current draft language of the standard seeks only a manual review of

#	Organization	Yes or No	Question 36 Comment
			the log rather than the manual verification of the logging capability.
36.16	Progress Energy - Nuclear Generation	Disagree	Incorporate information contained in the matrix in Attachment 1 for durations to ensure consistency by aligning CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
36.17	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
36.18	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring

#	Organization	Yes or No	Question 36 Comment
			that issue alerts for detected system events related to cyber security."Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.
36.19	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement R17 should be applied to both high and medium BES Cyber Systems.
36.20	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."Requirement R19 creates a potentially impossible level of

#	Organization	Yes or No	Question 36 Comment
			obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is presented to it.
36.21	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation 'Required for external connectivity only'.
36.22	American Municipal Power	Disagree	Please provide a little or no impact category
36.23	The United Illuminating Co	Disagree	R15.2, introduction of malicious code, responding to the introduction of malicious code is a specific cyber security incident. Suggest 15.2 be limited to processes to detect malicious code. Response is already part of cyber incident response.
36.24	Southwest Power Pool Regional Entity	Disagree	R15: Malicious code prevention is a basic security control and should be applicable to all impact categories. R17 and R19 should not make a distinction between external and non-external connectivity. R17: Once access is gained into the network by any means to any cyber system on the network, external access is immaterial.
36.25	Southern Company	Disagree	R19 comes from the DHS catalog, requirement 2.8.8. In the DHS catalog, there are 4 requirement enhancements, two of which are warnings which could greatly affect reliability. The DHS catalog presumes this requirement would be implemented on a case by case basis after appropriate research and testing. It therefore has no place in a mandatory standard that will force its use everywhere without regard to the reliability impacts. This requirement should be removed from a reliability standard.
36.26	National Grid	Disagree	Refer to answers in Q. 35.
36.27	Manitoba Hydro	Disagree	Requirement 18.4 can be very onerous for the industry for legacy systems which don't support automated log consolidation or review. The requirements must allow more flexibility.

#	Organization	Yes or No	Question 36 Comment
36.28	Garland Power and Light	Disagree	Requirement 19, 19.1 and 19.2 should not be required for any level
36.29	San Diego Gas and Electric Co.	Disagree	SDG&E feels that if R17.1 is a requirement for Medium Impact systems, then R17.2 should be as well for Medium Impact systems. For R18.3 and R18.4, SDG&E recommends that consistency be applied to the requirements to help ease the compliance burden of companies that have both High and Medium Impact BES Cyber systems. SDG&E also feels that instead of using the word "impact" for these Requirements, apply a concept of "risk" for inclusion. We would want to identify the risks with associated systems security and protect accordingly.
36.30	Con Edison of New York	Disagree	Section 15 & 16 should be limited to networked systems. Isolated microprocessors not part of a network should not have the same requirement.
36.31	ISO New England Inc	Disagree	see answer to question 35
36.32	Progress Energy (non-Nuclear)	Disagree	See comment 14.
36.33	WECC	Disagree	See comments for Q35Criteria should aplpy to all impact levels
36.34	LCEC	Disagree	See previous comments
36.35	BCTC	Disagree	See response to Q35.
36.36	Hydro One	Disagree	see response to Question 35
36.37	Entergy	Disagree	See response to Question 35 immediately above.
36.38	Northeast Power Coordinating Council	Disagree	See response to Question 35.

#	Organization	Yes or No	Question 36 Comment
36.39	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in rows 15.1, 15.2, 15.3, and 17.2. Suggest “Required for external connectivity only” for Medium Impact in rows 19.1 & 19.2.
36.40	Duke Energy	Disagree	Table 18: Manual reviews every 7 days is not practical.
36.41	Consultant	Disagree	Table R15 - Item 15.3 The requirement to "Implement processes to test and update malicious code protections." is confusing. Is the intent to "test malicious code protections and update malicious code protections" or to "test updates to malicious code protections" Please clarify the intent. There is a need to distinguish between updates to the malicious code protection "software" and malicious code protection "signature files". The software should be implemented in accordance with change control processes. The "signature files" are a specific subset of update to malicious code protection where it is unlikely a registered entity would have the capability to test what are typically vendor proprietary file formats. The extent of the 'testing' necessary for these signature files should be clarified.Table R16 - Item 16.2 While the concept of a "fixed date" sounds good, the requirement should allow for reasonable scheduling, including rescheduling, of the installation of applicable security patches or completion of mitigating measures. An option could be to remove the words "with a fixed date" and add a new item that would require that "Events that delay a security patch implementation schedule greater than thirty days shall be documented."Table R17 Item 17.1 The first sentence uses the terminology "network accessible ports and services" and the second sentence uses the terminology "network accessible services and communication methods". Suggest using consistent terminology to avoid confusion.Suggest defining the term "network accessible ports and services" (may be multiple terms) as they are intended for use in the standards. There does not appear to be a standardized definition for this term in the industry. The term "network accessible ports and services" appears to imply access across the protection boundary? If it does then the requirement statement of "Required for external connectivity only" is unnecessary and should be changed to "Required".Table R18 - Item 18.3 Suggest changing the word "within" to the word "for" for clarity of

#	Organization	Yes or No	Question 36 Comment
			meaning.Item 18.4 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 18.1 and 18.2 require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Table R19 - The limitation of these items to a Control Center is an added dimension of Impact that is not included in the impact categorization criteria. If data is an issue, then these requirement should apply to all assets based on impact categorization without addendum or modification by the requirement. Suggest modifying the impact categorization criteria to clearly identify those assets.Table R19 - "Inbound data" implies remote access, and the terminology "Required for external connectivity only" is redundant. Suggest changing the wording to "Required".Items 19.1 and 19.2 are inconsistent. Item 19.1 requires validation of inbound data, and item 19.2 provides an exception to validation for encrypted data. If you comply with item 19.1, then item 19.2 is irrelevant. If you comply with item 19.2, then you are in violation of item 19.1.R19 - Overall, this requirement should be removed in it's current form. Automatic system operation cannot exist if "inbound data" is required to be validated. Automatic system operation is dependent on responses to external data inputs. If the intent is to return the BES to manual operation, this requirement will achieve that end.
36.42	Alberta Electric System Operator	Disagree	Table R15 - make 15.1, 15.2, 15.3 required for Low Impact BES Cyber Systems, but possibly on a longer time horizon than for Medium and High Impact BES Cyber Systems.Table R16 - make 16.2 required for Low Impact BES Cyber Systems.Table R17 - make 17.1 “Required for external connectivity only” for Low, and “Required” for Medium and High. Make 17.2 required for Medium also.Table R18 - make 18.1 and 18.2 required for Low Impact systems. Make 18.3 90 calendar days for Low Impact systems. Make 18.4 30 calendar days for Low Impact systems.

#	Organization	Yes or No	Question 36 Comment
36.43	Idaho Power Company	Disagree	The review of logs every 7 days or even 30 days is extreme unless the logs are filtered for only abnormal events and only logs of abnormal events are reviewed.
36.44	Ameren	Disagree	The system hardening in Table for R17 is rendundant when other standards already restrict physical access to these systems.â€,â€,â€,R18.1, R18.2, R18.3, and R18.4 - Log file monitoring at Medium Impact Systems will be costly as there may not be bandwidth available to send the logs to a central location to be reviewed. Suggest removing these requirements for Medium Impact Systems.
36.45	Allegheny Energy Supply	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security.”Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.

#	Organization	Yes or No	Question 36 Comment
36.46	Allegheny Power	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: “Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security.”Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it.
36.47	EEI	Disagree	There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System

#	Organization	Yes or No	Question 36 Comment
			Components are already subject to physical protection requirements.Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."EEI recommends deleting R19. As written, R19, fails to recognize the obligation to "Do no Harm." Concerning data communication. Entities attempting to implement some of these measures, may in fact introduce latency or unintended, self inflicted denial of service attacks. It should be noted that the source of this requirement (DHS Catalog of Controls) provides multiple warnings about implementation risks associated with this control. It is not appropriate to put forth requirements that may reduce the reliability of the BES.
36.48	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
36.49	We Energies	Disagree	We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. In addition, the requirement should acknowledge that certain BES Cyber Systems may not be updated with security patches until the patches are certified for use by the vendor or integrator of the BES Cyber Systems. These requirements should be written in a manner to exclude a requirement for TFEs.We Energies agrees with EEI: The creation of a mitigation plan should not be deemed an exception requiring a TFE.We Energies agrees with EEI:

#	Organization	Yes or No	Question 36 Comment
			Requirement 17.2 does not add to the reliability of the BES. Externally accessible physical ports not needed for normal and emergency operations on BES Cyber System Components are already subject to physical protection requirements.We Energies agrees with EEI: Suggested change for overarching R18:Each Responsible Entity shall document and implement processes incorporating the criteria specified in CIP-011-1 Table R18 - Security Event Monitoring to collect and as appropriate, respond to security events on BES Cyber Systems that are able to detect and transmit such events.We Energies agrees with EEI: Requirement 18.1 needs to have refined requirements based on the characteristic of the devices to be protected. Not all BES Cyber Systems have the ability to capture or transmit cyber security logs. These requirements should be written in a manner to exclude a requirement for TFEs. The creation of a mitigation plan should not be deemed an exception requiring a TFE.We Energies agrees with EEI: Requirement 18.2 creates the need for 100% perfection regarding security monitoring. This is not appropriate. Suggest the following language for 18.2: "Implement and document one or more security processes for security monitoring that issue alerts for detected system events related to cyber security."We Energies agrees with EEI: Requirement R19 creates a potentially impossible level of obligation for responsible entities. The requirements should be more refined based on the characteristics and ability of the devices to be protected. Not every device has the ability to review or evaluate the data that is present to it. We Energies agrees with EEI: As written, R19, fails to recognize the obligation to "Do no Harm." Concerning data communication. Entities attempting to implement some of these measures, may in fact introduce latency or unintended, self inflicted denial of service attacks. It should be noted that the source of this requirement (DHS Catalog of Controls) provides multiple warnings about implementation risks associated with this control. It is not appropriate to put forth requirements that may reduce the reliability of the BES.
36.50	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R15 - R19:R15 Table 15.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR15 Table 15.2: Low

#	Organization	Yes or No	Question 36 Comment
			Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR15 Table 15.3: (If retained)Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR16 Table 16.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR16 Table 16.2: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR17 Table 17.1: Low Impact: N/AMedium Impact: Required for routable external connectivity onlyHigh Impact: Required for routable external connectivity onlyR17 Table 17.2: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for routable external connectivity onlyWe believe the “continuous security monitoring” as described in 18.2 is not practical for all BES Cyber System Components. We also believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally. Therefore we propose that for Medium impact facilities 18.1-18.4 be “Required for Control Centers only.”R18 Table 18.1: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: RequiredR18 Table 18.2: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: RequiredR18 Table 18.3: Low Impact: N/AMedium Impact: 90 calendar days for Control Centers OnlyHigh Impact: 1 yearR18 Table 18.4: Low Impact: N/AMedium Impact: 30 calendar days for Control Centers OnlyHigh Impact: 7 calendar daysR19 Table 19.1: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for external connectivity onlyR19 Table 19.2: (If retained)Low Impact: N/AMedium Impact: N/AHigh Impact: Required for external connectivity only

37. Requirements R20 to R22 of draft CIP-011-1 concern procedures for boundary protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R20 to R22? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note: CIP-011-1Requirements R20 through R22 have moved to CIP-005-5 Requirement R1.

Many commenters suggested phrases or aspects of the requirements that needed to be clarified. Several commenters questioned the need for weekly review of log entries, indicating that reviewing log entries at this interval would be burdensome with little or no positive impact on reliability.

Several commenters suggested reverting to the old name of Electronic Security Perimeter in place of Electronic Boundary Protection. In addition, several commenters suggested removing the system boundary protection requirement because it is overly prescriptive.

The drafting team agrees with commenters that some aspects of the requirement were too prescriptive, and has made significant changes to update the requirement both to clarify it and make it less prescriptive, while still addressing FERC Order 706 directives. The drafting team also agreed to revert to the Electronic Security Perimeter designation.

#	Organization	Yes or No	Question 37 Comment
37.1	WECC		Agree with concept, however, some work on the wording might make this more clear. R21 should have an additional item 21.3 - Cyber System components will not be shared with non-BES cyber systems or BES Cyber Systems of different impact levels.The former requirements for ESPs were better. The new language describing access points on communication paths may be an indirect way to get there, but it does not make things clearer or more auditable. This method of describing controls will make matters more complex and create additional work for entities.
37.2	GE Energy	Agree	"Logical Separation." Logical separation should be clarified. Logical separation could mean network access separation through an access point or it could be account separation by having separate user, system or service accounts that are different

#	Organization	Yes or No	Question 37 Comment
			amongst BES systems.
37.3	USACE - Omaha Anchor	Agree	Define 'unauthorized access attempts' is this a ping, or is this when a bad password is given to the system.
37.4	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.R20.20.2 - How does one implement a deny access by default for a dialup modem? That effectively either takes the modem out of service, or if you were to rely on the PSTN to do any kind of 'validation' of the incoming call, this is at best security through obscurity as it is trivial to spoof the callerid which is the only form of data validation that can be done over a dialup line.20.4 - What does "unauthorized access" mean? Does that mean an access attempt? Would a port scan of a firewall qualify as "unauthorized access"?20.5 - What does "unauthorized access" mean? If something as simple as a connection attempt qualifies, this requirement puts a tremendous burden on staff to track every little event that might happen on the firewall, and would not accomplish much in the end. If the intent of the standard is to keep unauthorized login attempts at bay, it should say that.R21.21.2 - Communication through an "electronic access point" for dial-up communications could prove difficult for some devices. Some devices are extremely sensitive to any sort of jitter introduced to a data stream, and having a security device in front of these kinds of devices may introduce enough jitter to make the communications unusable. R22.This seems duplicative of R14, R16, R18 and R23. FMPA suggest modifying those requirements to incorporate the protective cyber systems elements.22.2 - This should be consistent with R16; medium should be required to patch access control points. Also, low should have to patch at least quarterly. For access points, consider forcing high impact to asses 'critical' patches within 7 days.
37.5	Green Country Energy	Agree	Footnotes, guidance document?
37.6	Exelon Corporation	Agree	If systems are connected to a master station/location that is a BES Cyber system, do all the connected systems become BES Cyber systems? At what level do these

#	Organization	Yes or No	Question 37 Comment
			requirements apply - for example at the relay level where someone is logging into the relay? Exelon would like clarification on the definition of the electronic access point - is it at the component level or at the system level?
37.7	Progress Energy - Nuclear Generation	Agree	R20-22 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
37.8	Independent Electricity System Operator	Disagree	- R20.1 R20.4 20.5 and 20.6 External and External connectivity needs to be defined. External to BES Cyber System or components, boundary, connections with 3rd parties? What if multiple BES Cyber Systems are in the same boundary? - - R20.5 Please define
37.9	National Grid	Disagree	1. National Grid requests clarification on “all communication paths” in 20.1 which can be every possible communication path between two end points. The entity should be required to document only external communication paths with dial up access or routable protocol. Recommend removing R20.1 and 20.2 from LOW impact category.2. National Grid recommends removing “within the following time period” from 20.5 and 20.6. Also, for dial ups it would be difficult to review the alerts in the given time period. Suggest 30 days for logging related to dial-ups. 3. National Grid recommends that 20.6 be re-worded to be consistent with FERC Order P526 - “Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs.”4. National Grid recommends that 20.6 High Impact BES CS should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven days. Also should it be included for Medium Impact BES CS?5. National Grid recommends removing 21.2 since it is covered in 20.26. National Grid recommends removing R22 since it is redundant and move it’s table into the respective Requirements o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23

#	Organization	Yes or No	Question 37 Comment
37.10	Dairyland Power Cooperative	Disagree	20. What are the boundary rules for serial connectivity vs. routable protocols. Serial connections can be external to different systems and they can be internal. How do we determine if there is a boundary to protect?21. The logical separation rule needs more detail "Logical Separation" should have a definition. What is the impact for an RTU field device than can be scanned by multiple systems or entities? Is the mere configuration of available data on each physical or logical port enough to satisfy logical separation? What about components used as system-to-system gateways?
37.11	Regulatory Compliance	Disagree	20.1 - clarify - are these communication paths external to the electronic boundary?20.2 - clarify - This implies a firewall for even low impact?20.3 - guidance on what required elements to document20.6 - Clarify if this is for firewall logs only21.1 - Major clrification needed - what about BES Sytems that rely on input and out from system to system in having the logical separations?
37.12	Dominion Resources Services, Inc.	Disagree	20.1. The language "Document all communication paths" is too vague and suggests a need to map out the entire LAN/WAN infrastructure. Based on the May workshop discussion, the intent of the requirement is to document inputs and outputs associated with the BES Cyber System. Dominion recommends the following alternate wording for R20.1:"Document all digital interfaces associated with each BES Cyber System."20.4. Dominion recommends revising the language of this requirement to read:"Document and implement one or more processes for logging all access attempts at each electronic access point."Firewall logs cannot identify all "actual unauthorized access." Someone using a trusted source to gain access to a BES Cyber System would be permitted through a firewall. That is "actual unauthorized traffic" but it is not detectable. Blocked access attempts are shown in firewall logs as a dropped or denied entry.20.5. As explained in the comment for requirement 20.4, firewall logs cannot identify all "unauthorized access attempts." Therefore, Dominion recommends rewording this requirement to read as follows: "Document and implement one or more processes for alerting and review of alerts by designated response personnel at each electronic access point within the following time period."

#	Organization	Yes or No	Question 37 Comment
			20.6. Compliance with this requirement is labor intensive and, therefore, not practical for a large number of BES Cyber Systems. Requiring a manual review every 7 days is excessive for the benefit received and does not make allowances for reviewer unavailability due to sickness, emergency work or vacation. At minimum Dominion recommends extending the review requirement to every 30 calendar days or revising the requirement to allow for selected BES Cyber Systems to be reviewed every 7 calendar days as follows: "Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs for selected BES Cyber Systems within the following time period."21.1. The word "either" should be inserted after the word "provide." The phrase "or controlled access from one system to the other" should be added after "between each system." This modification is reflected in the revised language below: "Cyber System Components in Control Centers that are shared between BES Cyber Systems must provide either logical separation that prevents access between each system or controlled access from one system to the other."The issue is devices that provide a gateway between 2 systems. An example is the node that passes data between the EMS and ICCP networks.
37.13	Network & Security Technologies Inc	Disagree	20.2 - Current wording could be interpreted to mean an access point is required between a BES Cyber System and any other BES Cyber System the Responsible Entity may have defined, even if on a shared network. Could also be interpreted to mean access points are required on a per routable protocol basis. Assuming these interpretations were not intended, 20.2 should be rewritten for greater clarity.20.3 - Except for "document," this requirement seems to duplicate 20.2.20.6 - Wording suggests this requirement applies to all BES Cyber Systems. Is this what was intended, or is it to be applied to access point devices? Please clarify.21.1 - Please clarify intent and applicability of this requirement. Is it intended to apply to virtual machines? Disk arrays shared by multiple application servers? Both? Neither?21.2 - Redundant if all access points are properly identified. Suggest eliminating it or combining the statement with one of R20's sub-requirements.R22 - Seems to overlook physical protections for cyber systems that establish electronic boundaries.22.4 - Configuration changes such as updating access control settings on a firewall or

#	Organization	Yes or No	Question 37 Comment
			revising the physical access permissions associated with a card key should not be subject to this requirement, and it should so state.
37.14	American Electric Power	Disagree	20.2 & 20.3: Regarding "Document and implement access control at each electronic access point established in Part 20.2", is this redundant to R14 - lines 14.1 through 14.3? Suggest rewording or removing if it poses double jeopardy.20.6: Regarding "Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs for each BES Cyber System within the following time period", does this provide any security benefit? If a system event for cyber security was missed by an automated tool, is it reasonable to expect it to be found in a manual review? What is an entity supposed to look for in this manual review?21.2: Regarding "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20", it appears that this is a restatement of the elements of R20. If that is not a correct assumption, the SDT need to provide additional information.
37.15	ERCOT ISO	Disagree	20.2: Recommend using “ingress or egress point” instead of “access point”. 22.1-22.3: Please remove reference to other standard. Address the content in the appropriate standard only. The circular references in the existing standards are very difficult to navigate and provide opportunity to miss the requirement.
37.16	BGE	Disagree	20.5 timeframe should be consistent for medium and high.
37.17	Alliant Energy	Disagree	Alliant Energy agrees with the EEI comments.
37.18	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
37.19	Southwest Power Pool Regional Entity	Disagree	Clarify the requirement. A reader could interpret the criteria as requiring an access point between each defined BES Cyber System regardless of network segment placement. 20.4: More often than not, authentication is performed at the end host

#	Organization	Yes or No	Question 37 Comment
			system. Rather than prescribing logging of attempted or actual unauthorized access at the access point, simply require such logging at the point such unauthorized access is detected. 20.6: What are the minimum expectations for a log sampling program (e.g., how much, how often?). 21: Clarify that shared BES Cyber System Components (e.g., a networked storage device) must be afforded the highest impact categorization of all of the BES Cyber Systems sharing the component (similar to the sharing aspect of the electronic access point definition). 22: Include the requirement to protect the access control system from unauthorized physical access.
37.20	CenterPoint Energy	Disagree	Disagree - R20.2 CenterPoint Energy suggests striking the word dial-up. If dial-up is not stricken a TFE may be required to comply with this requirement for serial dial-up paths.CenterPoint Energy believes requirements, R20.3-R20.6, may require a TFE for compliance for non-routable protocols.R20.6 CenterPoint Energy believes the 7 day calendar requirement to review sampling of log entries is overly burdensome and unnecessary. Controls and alert processes to notify appropriate personnel of unauthorized access attempts are mandated in prior requirements. CenterPoint Energy recommends a 30 day review.
37.21	E.ON U.S.	Disagree	E.ON U.S. interprets R20.1 to require documentation of “all” communication paths which could include communication links to all RTUs, etc. This level of documentation is not necessary
37.22	Duke Energy	Disagree	Elimination of terms such as electronic security perimeter without a completely thought through substitute concept contributes to industry frustration. The industry, at least, had come to understand the concept of an ESP. How the “boundary” is identified does not seem well thought through. In the text box, information such as “...cyber systems sharing one or more common electronic access points ...will be treated at the highest BES Cyber system impact categorization level of the BES Cyber system...” seems to belong in CIP 010 where the actual categorization occurs. This information is NOT a technical control and does not seem to belong in CIP 011. Rather it provides additional information concerning the categorization. This standard

#	Organization	Yes or No	Question 37 Comment
			will cause entities to document a lot of confidential information, which then must be protected. R20 - electronic security perimeter is a retired term, suggest replacing with a different term.Table 20: 20.2 is confusing for initial setup processes. How can we explicitly authorize?Requirement 20.2: The electronic access point can therefore be shared between systems as defined in the text box beside R20. For generation stations in particular, there are many connections between equipment that are required/desired for the plant to operate (e.g. feedwater control system to the plant process computer in a nuclear station). Sharing such an access point is highly desirable. Requirement 20.2, as written, seems to contradict the definition in the text box in requiring that the Responsible Entity establish an electronic access point on EACH routable protocol or dialup communication path between BES Cyber Systems.Requirement 20.4: this requirement makes sense if remote/external access is defined by the "shared access point" as described here (which seems to be in agreement with comments made in sections R11, R12, R13, where the emphasis was on communication between the devices rather than "at the access point").Requirement 20.6: please consider including the words "related to electronic boundary protection" to make the sentence read as follows: Document and implement a process for manual review of a sampling of log entries or sorted or filtered logs relating to electronic boundary protection for each BES Cyber System within the following time period. Also, where logs are accumulated, there is no way to tell if the user was internal or external to the edge device.Table 2121.1 Suggest changing 'prevents' to 'limits' or remove 'that prevents access'. Within Generation, that access is required. Also, Does "logical separation" include "virtual separation"?21.2. Verify this is not just for control centers.
37.23	RRI Energy	Disagree	For 20.1, define communication path, eg., source and destination(s) only or everything in between?For 20.5, what does "all unauthorized access attempts" mean? If an operator fat-fingered login password, does the standard expect alert and follow up each time? "all unauthorized access attempts" needs to be redefined with some threshold before declaring it as unauthorized access attempt. Otherwise, Entities and operators will spend a lot of time documenting unauthorized access and instead of

#	Organization	Yes or No	Question 37 Comment
			securing their assets.
37.24	Northeast Utilities	Disagree	For 20.5, please provide clarification on the meaning of "all unauthorized access". Every password violation for example, is not an unauthorized access attempt but could be interpreted as such. Do we really need to follow-up on every invalid password attempt? Instead of every invalid password attempt, are password lockouts an appropriate trigger? Also, please consider addressing repeated lockouts in the criteria specified.R22 appears to be significantly weaker than the previous standards. One area that is specifically weaker is with regard to access control to Protective Cyber Systems. How can an entity not authorize, review and revoke a role as important as a firewall administrator?
37.25	Constellation Power Source Generation	Disagree	In R20.1 as well as the definition box, the term digital information needs to be defined further. R21 inherently forces entities to further segment their BES Cyber Systems, which is counter to the entire premise of allowing the entities to define their own BES Cyber Systems. Allowing the entities to define their own BES Cyber Systems would limit the scope of an attack, which the SDT stated in the CIP V4 Workshop as their goal in R21. Constellation suggests removing this requirement entirely. Likewise, R22 should be removed as it is completely redundant. Note that in each sub requirement it merely points to another requirement in the document. A suggestion would be to implement the verbiage found in Table R22 to each of the requirements it points to.
37.26	Alberta Electric System Operator	Disagree	In Table R21, was the intent of 21.1 only for Control Centers? The AESO would suggest removing the Control Center parameter and make 21.1 applicable to all High and Medium BES Cyber Systems.
37.27	Constellation Energy Commodities Group Inc.	Disagree	Is the intent to require use of hardware firewalls? If so, is it possible to state that clearly? If not, what is the intent?
37.28	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).

#	Organization	Yes or No	Question 37 Comment
37.29	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's observations below:Suggest using electronic security perimeter rather than “Boundary Protection.”Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than “System Boundary Protection.”Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for “Protective Cyber Systems” to include remote access controls, patch management, security event alerting, change control and change management.
37.30	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R20, but recommends changes as follows: o Regarding Part 20.2, since Low Impact BES Cyber

#	Organization	Yes or No	Question 37 Comment
			Systems do not require any Physical Security as defined in previous requirements, it seems inconsistent to require electronic access point security for those systems. o Regarding Part 20.4, how does the Standards Drafting Team envision that a Registered Entity would log "actual unauthorized access?" Actual unauthorized access is not identifiable since it would appear to have been authorized (or the attempt would not have succeeded. o Regarding Part 20.4, in reading and applying the definitions of "remote access" and "external connectivity," remote access is a specific type of external connectivity. Therefore, any reference to criteria for remote access based on whether or not it is externally connected is redundant. o Is it the Standards Drafting Teams intent that Part 20.5 require an after the fact review of unauthorized access attempts? If so, it may not be possible to adhere to proposed timeframes, especially in instances where BES Cyber System support is 8 hours a day, 5 days a week. If it is the Standards Drafting Teams intent that Part 20.5 address responding and monitoring a potential malicious attack situation, then the time frames are not sufficient.Minnesota Power generally agrees with the proposed Requirements R22, but recommends changes as follows: o The language in Part 22.1 creates confusion. The requirement states that remote access is to be restricted as stated in R14 and that for Low Impact BES Cyber Systems this is required. However, in reviewing Requirement R14, only Part 14.1 is required for Low Impact BES Cyber Systems. As a result, does this mean that only Part 14.1 needs to be implemented for Low Impact Cyber Systems in 22.1 or do 14.1-14.4 need to be implemented? The same should be addressed for Medium Impact BES Cyber Systems. o The same type of confusion regarding the language in Part 22.1 exists in Parts 22.2, 22.3, and 22.4. The Standards Drafting Team should consider whether these cross-references are necessary. It does not appear that Parts 22.1-22.4 are identifying specific criteria, but rather are a reminder that these assets need to comply with R14, R16, R18, and R23.
37.31	NextEra Energy Corporate Compliance	Disagree	NextEra believes requirement 20.1 is unclear as written. Is the communication path expected to end at each and every end point that receives digital information to each BES Cyber System? If this communication path is to each end point, it would be difficult to demonstrate compliance. Does compliance to this requirement also

#	Organization	Yes or No	Question 37 Comment
			require all the communications paths within a WAN or ISP?Requirement 20.2 does not allow a responsible entity to put more than one BES Cyber System inside an access point since it requires access points between systems. This is highly inefficient and creates access points where not needed and could potentially impact the reliability a BES Cyber System. It is unclear why the requirements are moving away from the well established ESP concept. This concept is well established in 'defense in depth' and other security frame works. The requirements for boundary protection should follow the ESP model from V1 and V2 of the NERC CIP requirements. In addition the definition also (inadvertently) conflicts with the definition given at the start of this requirement related to access points and therefore is open to interpretation by auditors.Requirement 20.4 requires the documentation and implementation of one or more "processes for logging of all authorized remote access and all attempts at or actual unauthorized access at each electronic access point." Until the definition of remote access is clearly defined, it is unclear how responsible entities must comply and demonstrate compliance. In addition, it is unclear if remote access is considered any an access attempt from outside of the access point.Requirement 20.5 requires, "Document and implement one or more processes for alerting and review of alerts by designated response personnel on all unauthorized access attempts at each electronic access point within the following time period." The responsible entity should be able to determine the threshold for unauthorized access attempts. The way the requirement is written now, personnel would have to investigate every single denied access attempt including someone who accidentally fat fingered their credentials when trying to gain authorized access to a BES Cyber System component. The recommended approach would be to require a review of 4 or more failed attempts against a common UserID without a successful login within 1 hour. Also consider more than X total bad access attempts within one hour for User ID brute force attacks or reconnaissance. Also, in 20.1, please define what is meant by the word "paths" Is it logical or is it physical path?In 20.4, is a single failed login classified as an attempt? The wording states "all attempts at or actual unauthorized access at each electronic access point"In 21.1, does this mean that for example, a SAN

#	Organization	Yes or No	Question 37 Comment
			(Storage Area Network) can be shared by Cyber System Component and other devices as long as there is logical separation?In 21.1, if two BES Cyber Systems "share" a network switch, does this meet the requirement of "logical separation"?
37.32	PacifiCorp	Disagree	PacifiCorp agrees with EEI's observations below:Suggest using electronic security perimeter rather than “Boundary Protection.”Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than “System Boundary Protection.”Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for “Protective Cyber Systems” to include remote access controls, patch management, security event

#	Organization	Yes or No	Question 37 Comment
			alerting, change control and change management.
37.33	Puget Sound Energy	Disagree	Puget Sound Energy has the following comments:R21.1 - Puget Sound Energy has concerns that Cyber System Components that are shared between BES Cyber Systems must provide logical separation. For example: For entities with Control Centers that utilize a Microsoft infrastructure, multiple BES Cyber Systems may centrally authenticate (or have logical security controls) facilitated by a single or clustered Microsoft Active Directory domain controller. As the requirement is currently written, Puget Sound Energy feels that those shared domain controllers would not be able to reside on the same local area network segment as the domain they participate in. Puget Sound Energy requests clarity be added in to this requirement.Table 22 - Puget Sound Energy suggests including "Where Technically Feasible" to R22, as some Protective Cyber Systems may be incapable of meeting all the requirements in Table 22.Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, Table 14, and Table 22. Puget Sound Energy suggests including wording similar to Table 11: "Required for external connectivity only".
37.34	LCEC	Disagree	R20 - 20.1 Must define what is included in communication paths. If needed specify physical interface. Digital information is actually digital data, control, or signals.20.3 is not auditable. What is access control. There is no defined scope.20.5 includes requirements for cyber incident response which is covered in a later requirement.Need to clearly identify what is considered an access point on multiple interface devices.20.6 what's the difference between this and 18.4?21.2 A BES Cyber System could include components at different physical locations that communicate with each other. This is not technically external to the system so does it apply here?
37.35	FirstEnergy Corporation	Disagree	R20 - 20.6 - Need greater clarity around whether automated alarming can be used rather than manual review of logs. This sub requirement is unnecessary with an automated system in place.R21 - We agree with the use of 'logical separation' in this requirementR22 - We do not like the way R22 refers back to other requirements. This

#	Organization	Yes or No	Question 37 Comment
			is redundant and the requirement should be eliminated.
37.36	Consultant	Disagree	R20 - The terminology appears to be incorrect. Electronic access points do not define an electronic security perimeter. It also seems odd to say the defined term Electronic Security Perimeter is going to be retired, and then use that same term to define a requirement. "Electronic Boundary Protection" is created by identifying an electronic security perimeter based on the logical network connections of cyber assets, which includes electronic access points for External Connectivity that provides Remote Access to the assets within the electronic security perimeter. Suggest retaining the term Electronic Security Perimeter as described here.Table R20 - Items 20.1 & 20.2 - This appears to be "Identifying the Electronic Security Perimeter" as describe in the comment above regarding the usage of the term Electronic Security Perimeter, but stated in more confusing language in both cases.Item 20.3 Suggest rewording as "Implement and document access control mechanisms for each electronic access point (to the Electronic Security Perimeter)."As a general comment you would "implement and document" rather than "document and implement"Item 20.4 Suggest rewording as "Implement and document access attempts and access authorizations at each access point." Item 20.4 - The terminology "Required for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest changing to "Required"Item 20.5 contains two requirements:1. Implement and document processes to identify unauthorized access attempts at each electronic access point.2. Responsible entities shall review unauthorized access attempts in the time frame specified.Item 20.4 - The terminology "Required for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest changing to "48 hours" & "12 hours".Item 20.4 - It would appear to create an excessive administrative burden without corresponding decrease in risk to require this review every 12 hours for High Impact Assets. Suggest changing required review time to "Daily".Item 20.6 - The requirement statement is subjective in regard to the degree of sampling, sorting, and filtering allowed, expected, or required. This is a requirement similar to event log review of Table R18 - Item 18.4 and the wording of these two requirements should be similar.Item 20.6 -

#	Organization	Yes or No	Question 37 Comment
			This requirement is regarding access through electronic access points and "7 calendar days for external connectivity only" is redundant. Suggest deleting "for external connectivity only"Item 20.6 - Weekly log review appears to create an excessive administrative burden without a corresponding decrease in risk to the High Impact assets. Items 20.4 and 20.5 (as commented) require continuous monitoring of the same activity. Manual log review is redundant to these requirements. While there may be a reason for manual log review to confirm the continuous monitoring is occurring as expected a more reasonable periodicity of monthly or quarterly should be required for both Medium and High Impact assets.Items 20.1, 20.4, & 20.5 - Delete the word "all" It is redundant and unnecessary to the requirement statement. (The word "all" should be removed from "all" requirement statements in the standard")Table R21 - Item 21.1 This requirement appears to create a mutually exclusive situation where shared cyber system components are separated. The wording needs to be clarified or, as it is worded it should be deleted.Item 21.1 The application of the requirement to control centers creates an added dimension to the impact categorization. The application of requirements is based on impact categorization. Modify the impact categorization criteria to capture the assets where this requirement should be applied.Item 21.2 This item appears to restate what is previously stated in the referenced R20. If some additional requirement is intended, then that requirement should be included in the reference R20 requirements list, rather than a 'hidden' requirement that is cross-referenced here.R22 - This requirement appears to be redundant. The requirements referenced in the Table R22 (R14, R126, R18, & R23) appear to include whatever is listed in this requirement. If there is some additional requirement that is intended, that requirement should be put in the respective referenced requirements. Each requirement statement and table should be contain everything related to that requirement, rather than having a separate requirement that 'adds' to other requirements.
37.37	Xcel Energy	Disagree	R20.1 - The definition and level of detail for “communication paths” is needed. For example, does this include a commercial telephone carrier used to communicate between relays?R20.2 - Clarifying language is needed for “Establish an electronic

#	Organization	Yes or No	Question 37 Comment
			access point". Does this mean in documents, drawings, etc?R20.5 - This requirement needs clarification. Are these intended to be automatically generated alerts, such as logs? The current language could be interpreted to require a 12 hour review of a login attempted that failed due to an incorrectly typed login ID, as automated software may interpret this as an authorized login attempt. Also, 12/48 hours to complete a review of a failed unauthorized login attempt is unreasonable and unnecessary. R21.1 - We would like additional information on what type of "logical separation" is expected.
37.38	Ameren	Disagree	R20.1 - This will require use of a firewall at all locations or similar devices. Simply documenting this information is not practical for non routable devices. Also, clarify if communication paths, refer to physical equipment or locical paths. R20.2 - What is the difference between R20.2 and R20.3? Suggest combining the two requirements.R20.5 - 12 hours does not allow for weekends or for events that occur outside business hours. This should be increased to 24 hours or lowered to 24x7 (continuous). Also, need to clarify whether the alerts need to be reviewed during the time frame given (48 hours, 12 hours, or 7 days) or that alerts need to be sent every 48 hours, 12 hours, or 7 days. Please clarify how often should alerts be sent and how often do they need to be reviewed. R21.2 - Where does an RTU or serial communication fit into this requirement? Need to add more clarification on this requirement of what devices are included. R22 - Need to add requirements at a minimum for account listings, approvals, and access controls. There are no considerations for risk assessment or training for users of these devices. Also, these devices should be included in the Vulnerability Assessment.
37.39	US Bureau of Reclamation	Disagree	R20.2 should be modified to read "Establish an electronic access point on each routable protocol or dialup communication path between BES Cyber Systems." Define the use of "other devices" in this context. R20.4 - add "where feasible" to this requirement.R21.2 - Please provide and example...

#	Organization	Yes or No	Question 37 Comment
37.40	Entergy	Disagree	R20.5 Entergy cannot understand the reasoning behind the criteria of 12 hours? Why not 6 or why not 24?R21.1 is unclear and must be reworded to better reflect exactly what the SDT had in mind. We cannot guess at what that might have been.R22 - Entergy suggests R22 apply equally for high, medium and low assets; and thatthe requirements for processes and procedures in this section should be placed back into each of the respective sections (R14, 16, R18 and R23).
37.41	Western Area Power Administration	Disagree	R20.6 - Is this a requirement to review, and document the review, of logs weekly?R21.2 - Unclear. Does it mean our "one-way" rule from internal to external? Or does it mean use a proxy located outside the ESP?
37.42	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R20.6. With the obligation of reviewing alerts designated in R20.5 the requirement for manual review of logs should be extended to a 30 day window.
37.43	BCTC	Disagree	R22. Suggest just removing this requirement as it just references previous requirements
37.44	Hydro One	Disagree	Request clarification on “all communication paths” in 20.1 which can be every possible communication path between two end points.Recommend removing R21 because: o 21.1 is prescriptive in requiring Entity’s to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move its table into the respective Requirements: o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23
37.45	ISO New England Inc	Disagree	Request clarification on “all communication paths” in 20.1 which can be every possible communications between two end points20.3 should be part of 20.2 - denys and explicit allows might be better language. R20.5 Please define what is an unauthorized access attempt. A user may be authorized but may try to connect using telnet where telnet is disabled. Is this considered unauthorized? Recommend

#	Organization	Yes or No	Question 37 Comment
			removing R21 because: o 21.1 is prescriptive in requiring Entity's to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move it's table into the respective Requirements o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23R21.1 = question on what is "logical separation" very vague
37.46	Northeast Power Coordinating Council	Disagree	Request clarification on "all communication paths" in 20.1 which can be every possible communication path between two end points.Recommend removing R21 because: o 21.1 is prescriptive in requiring Entity's to segment their BES Cyber System o 21.2 is covered in 20.2Recommend removing R22 and move its table into the respective Requirements: o Move 22.1 into R14 o Move 22.2 into R16 o Move 22.3 into R18 o Move 22.4 into R23
37.47	Oncor Electric Delivery LLC	Disagree	Requirement 20.4, 20.5 and 20.6 are not applicable to some legacy cyber systems. These requirements should only be required for systems which utilize routable communication.Requirement 22 references other requirements and should be eliminated because it is redundant.
37.48	Garland Power and Light	Disagree	Requirement 20.6 - What we really feel is that this is impractical and should be deleted. However, it was stated at the NERC CIP workshop that the intent was to verify that the automated system capturing various logs off cyber devices was actually capturing each log - intent needs to be added to the requirement or wording changed to better express the intent at a minimum. Requirement 22 - Keep life simple - add the words "and Protective Cyber Systems" after the words BES cyber systems in each of the referenced requirements (14, 16, 18, and 23) and DELETE Requirement 22 - that way, everything is covered by the referenced requirements that this R22 uses
37.49	San Diego Gas and Electric Co.	Disagree	SDG&E feels that R20.1 is not clear. What is the point of documenting paths that transmit or receive digital information external to each BES Cyber System if they may not interface with other BES Cyber Systems? In addition, another observation from SDG&E related to R20.1 has to do with non-routable protocols. If this requirement

#	Organization	Yes or No	Question 37 Comment
			includes the documentation of non-routable protocols, it can become VERY expensive to document "chatty" protocols that broadcast to lots of assets (DHCP and BOOTP, to name just two examples).In R20.2, SDG&E asks for a clarification of the term "explicitly".SDG&E recommends grammatical changes for R20.4. We feel it should read "Document and implement one or more processes for logging all authorized remote access sessions and all successful and unsuccessful attempts of unauthorized access at each access point within the following time period. SDG&E suggests the following changes to R20.5: "Document and implement one or more alert processes that includes review of alerts by designated response personnel..." SDG&E feels that R21.1 is a bit confusing and worthy of discussion. If affected cyber systems and components are on the same network anyway, then what are the benefits of logical separation?
37.50	Allegheny Energy Supply	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection." (In general, using the existing terms where possible will cause much less confusion.)
37.51	Allegheny Power	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection."
37.52	EEI	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection."Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.For R 20.5: Document and implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.For R 20.6: Document and implement a process for

#	Organization	Yes or No	Question 37 Comment
			manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.R21: Suggest using electronic security perimeter rather than "System Boundary Protection."Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.There may need to be additional requirements for "Protective Cyber Systems" to include remote access controls, patch management, security event alerting, change control and change management.
37.53	Progress Energy (non-Nuclear)	Disagree	Suggest using electronic security perimeter rather than "Boundary Protection." Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.Is the relay communications port for local interface with a laptop considered as an electronic access point? If so, this complicates these requirements.R20.1 by external to each BES system do you mean outside individual six walled boundaries?R20.6 is not needed, as long as we do R20.5.For 20.5 - Don't see the need for more than one capability.For 20.6 - change to "document process to ensure automatic monitoring and alerting process is working properly"CIP-011 - R20 - Are communications between Control centers and field RTUs/IEDs which do not employ routable protocols considered remote external communications?R20.6 - Need additional guidance as to what constitutes a manual review and the minimum sampling required.CIP-011 - R21 - Need clarification with guidance as to what constitutes "Cyber systems components in control Centers that are shared between BES Cyber Systems"

#	Organization	Yes or No	Question 37 Comment
37.54	Detroit Edison	Disagree	Table entries 20.4, 20.5, and 20.6 specify external connectivity only. This text is not necessary since the requirement is boundary protection and that implies external connectivity is the scope.
37.55	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments on this question, but also provides the following drafting suggestions:R20. Objective:To define an electronic security perimeter thereby minimizing the risk of system intrusion.R20. Requirement:Each Responsible Entity shall document and implement processes that establish electronic access controls point that incorporate the criteria in CIP-011-1 Table R20 - Electronic Boundary Protection. In R20 Table 20.2 we are concerned about the term “explicitly authorized communication.” It is our assumption that a password is sufficient to comply with this requirement. If the drafting team intended another meaning we believe this will not be reasonable and we could not support this definition. We propose the following revised language:Table 20.2: Establish electronic access control on each routable protocol or dialup communications path between BES Cyber Systems and other devices.We recommend that R20 Table 20.4 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. We recommend that R20 Table 20.5 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. We recommend that R20 Table 20.6 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. R21. Objective:To protect each BES Cyber System from other cyber systems by establishing protected boundaries between each cyber system and any shared components. R21. Requirement:Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R21 - System Boundary Protection. The APPA Task Force supports the MRO-NSRS proposal to delete criteria in R21 Table 21.2. This is a redundant requirement and would put an entity in noncompliance of 2 requirements for one violation. The APPA Task Force recommends removal of R22. All of the criteria in Table 22.1 - 22.4 refer to previous requirements and will put an entity in noncompliance of 2 requirements for one violation.

#	Organization	Yes or No	Question 37 Comment
37.56	Bonneville Power Administration	Disagree	The objectives of these requirements ("to define an electronic security perimeter thereby minimizing the risk of system intrusion," "to protect each BES Cyber System from other cyber systems by establishing protected boundaries between each cyber system and any shared components," and "to protect each cyber system that establishes physical or electronic boundaries of BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirements rather than appearing at the end of the requirements (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R20Section 20.1 This is unacceptable. The requirement does not limit the extent of the documentation. Conceivably, it could require documentation of the entire Internet, if the BES Cyber Asset had direct or even indirect access to the Internet. The requirement needs to be limited. Recommendation: Remove the requirement. It is difficult to see how to write it in a way that encompasses all possibilities without leading to results such as the one described above. Instead, document external interfaces as part of the configuration management process.20.2: Requiring an electronic access point between a BES Cyber System and any other system produces unacceptable complication, latency, and administrative burden for a facility with multiple BES Cyber Assets in close proximity. As an example: 20.2 would require that all traffic from one BES Cyber System within a Control Center to any other system within the Control Center to go through a firewall or some other access control device. It is unlikely that this was the intent of the entry. Recommendation: Replace "Required" with "Required for external connectivity only", using the redefinition of external connectivity described above.20.3 Similar issue to 20.2 Recommendation: Replace "Required" with "Required for external connectivity only" throughout the table.20.4 - 20.6. Remove, the are already covered under 18.3 and 18.4. R18 and Table R18 require monitoring of all cyber security events, whether at access points or at BES Cyber Systems themselves.20.6. First, the requirement is already covered more clearly in Table R18. Second, it is unclear why a Electronic Boundary Protection requirement should be addressing BES Cyber Systems. Third, The intent is unclear,

#	Organization	Yes or No	Question 37 Comment
			due to the plethora of "ors" in the requirement. It could be that a manual review is always required, using sampled, sorted or filtered logs. It could also be that a manual view of logs is required, using sorted or filtered logs. It could also be that either a manual review or {sorted or filtered logs} is required. Part of the confusion is that filtering is clearly a method to sample, and sorting may be, as well. It would probably be better not to use those terms at all. In addition, there should be a provision to allow automated review of log entries. Recommendation: Delete the entry.Table R21Section 21.1 is completely unacceptable. It is quite possible in a Control Center for a single Dispatch workstation to provid access to several BES Cyber Systems. The requirement in 21.1 would make this impossible. The alternate would be to provide a separate workstation for each such system, which is unacceptable.Section 21.2 is acceptable only with externally connected redefined as described above.R22 and Table R22: These are references to other requirements. It seems that rather than referring to the other standards from this one, it would be cleaner to simply include this requirement as part of those other standards. That is, put the necessary references in R14, R16, R18 and R23.
37.57	Constellation Energy Control and Dispatch, LLC	Disagree	The timeframe in 20.5 for medium and high should be the same.
37.58	ReliabilityFirst Staff	Disagree	To eliminate confusion, we believe the drafting team should develop a definition for “protective cyber system”. We also believe that Table R22 should include an additional requirement stating, “Implement processes as specified in Requirement R15 - System Security.” and make this new requirement TFE eligible. Further, this new requirement should be “Required” for medium and High Impact BES Cyber Systems.
37.59	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
37.60	American Transmission	Disagree	We believe item 20.2 is going to set the stage for numerous TFE’s within the industry. Many devices (i.e., protective relays) do not support explicitly authorized

#	Organization	Yes or No	Question 37 Comment
	Company		communication.We believe items 20.4 - 20.6 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. These items do not appear to be applicable for non-routable connections, and adding this language would assure they are limited to routable and dialup connections only.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.61	MRO's NERC Standards Review Subcommittee	Disagree	We believe item 20.2 is going to set the stage for numerous TFE’s within the industry. Many devices (i.e., protective relays) do not support explicitly authorized communication.We believe item 20.4 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only.We believe item 20.5 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only.We believe the following should be added to the end of item 20.6: “at each electronic access point established in Part 20.2”. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only. It also makes for a consistent approach with item 20.3.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs

#	Organization	Yes or No	Question 37 Comment
			non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.62	The Empire District Electric Company	Disagree	We believe item 20.2 is going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicitly authorized communication.We believe items 20.4 - 20.6 should specify "at each electronic access point established in Part 20.2", similar to item 20.3. These items do not appear to be applicable for non-routable connections, and adding this language would assure they are limited to routable and dialup connections only.Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.
37.63	We Energies	Disagree	We Energies agrees with EEI: Suggest using electronic security perimeter rather than "Boundary Protection."We Energies agrees with EEI: Suggest changing R20.1 to: Document all communication methods including authentication measures used to connect devices that transmit and/or receive digital information external to each BES Cyber System.We Energies agrees with EEI: There needs to be more refined requirements based on the characteristic of the devices to be protected. Dialup communication path should be defined for clarity.We Energies agrees with EEI: Requirement 20.4 creates the need for 100% perfection regarding remote access monitoring. This is not appropriate. Suggest the following language for 20.4: We Energies agrees with EEI: Document and implement one or more processes for logging of authorized remote access and attempts at or actual unauthorized access at each electronic access point.We Energies agrees with EEI: For R 20.5: Document and

#	Organization	Yes or No	Question 37 Comment
			implement one or more processes for alerting and review of alerts by designated response personnel to unauthorized access attempts at each electronic access point within the following time period.We Energies agrees with EEI: For R 20.6: Document and implement a process for manual validation that ensures that log events are being collected. This review can include of a sampling of log entries or sorted or filtered logs for a sampling of BES Cyber System within the following time period. We Energies agrees with EEI: Not every BES Cyber System has the ability to create or transmit log entries. This requirement should not create the need for TFEs.We Energies agrees with EEI: R21: Suggest using electronic security perimeter rather than "System Boundary Protection."We Energies agrees with EEI: Requirements R21.1 and R21.2 only make sense for components that use a routable protocol. This should be made clear. We Energies agrees with EEI: R22 Needs to include additional scoping language to include or exclude certain devices. For example, proximity card readers may not have any physical protection, but are an integral part of an overall physical security solution.We Energies agrees with EEI: Suggest breaking up requirements associated with the electronic security of systems from the physical security of systems.We Energies agrees with EEI: There may need to be additional requirements for "Protective Cyber Systems" to include remote access controls, patch management, security event alerting, change control and change management.
37.64	GTC & GSOC	Disagree	We recommend rewording R21.1 to provide clear direction on what is expected to comply with this requirement because the wording is ambiguous. We are unable to suggest alternative language because we are not certain of the intent. If this requirement would prevent, for example, the use of a shared backup system for two Cyber Systems we do not see the reliability based justification for the requirement and would recommend its elimination.
37.65	Emerson Process Management	Disagree	What is the difference between "Electronic Access" in R20-R22 and the "Remote and Wireless Electronic Access" in R11-R13?

#	Organization	Yes or No	Question 37 Comment
37.66	Manitoba Hydro	Disagree	What is the meaning of "dial-up"? The wording for Requirement R20.2 is unclear. The suggested wording for Requirement 20.2 is "Establish an electronic access point that denies access by default and allows explicitly authorized communications on each routable protocol or dial-up communication path between BES Cyber Systems and other devices. Requirement R20.2 is inconsistent with Requirement R20.3. It is unclear how explicitly authorized communication is allowed without the implementation of access controls for Low Impact BES Cyber Systems. Requirement R20 does not contain any requirement for response to alerts. The wording for Requirement 21.1 is unclear. The suggested wording for Requirement 21.1 is "Cyber System Components that are shared between BES Cyber Systems must provide logical separation that prevents access between each system." and change the wording in the impact columns to "Control Centre Only". The wording for Requirement R21.2 is unclear. The suggested wording for Requirement R21.2 is "All external communication to the BES Cyber System must occur through an electronic access point as specified in Requirement R20." Requirement R22 is missing the requirement for the physical protection of the cyber system that establishes the physical or electronic boundaries of the BES Cyber System. There are no specifics given with respect to 'logical' separation in Requirement R21.1 so it is assumed to be at the Responsible Entity's discretion to determine.

38. Do you agree with the proposed definition of electronic access point? Please explain and provide any suggestions for modification.

Summary Consideration:

Many commenters agreed with the definition of Electronic Access Point, but other commenters requested clarifications in the definition. A number of commenters recommended changes to language concerning systems sharing an electronic access point. Some commenters suggested removing the sharing of electronic access points from the definition.

In response, the SDT has modified the definition of an **Electronic Access Point** to: *"An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets"*.

The sharing of electronic access points is likely not an issue because High Impact BES Cyber Systems are Control Centers and would rarely share an Electronic Access Point with Medium Impact BES Cyber Systems.

#	Organization	Yes or No	Question 38 Comment
38.1	WECC		Move to definition to beginning of the standard; dislike the definition box in the middle of a requirement. Make clear that access points can be anything that meets the definition and not only firewalls or devices specifically created for this purpose that must be put "in line". Ie. an Access Point can be the actual device itself providing access control.The phrase "where electronic access can be controlled" will prove difficult to audit. Inherently it allows an exception. All communication paths should be in scope regardless of the ability to control electronic access. It is not foreseen that communication paths could not be controlled.
38.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
38.3	NextEra Energy Corporate Compliance	Agree	Is a serial connection to a BES Cyber System considered an electronic access point? Please clarify in requirements.
38.4	Minnesota Power	Agree	Minnesota Power agrees with the proposed definition of electronic access point, but recommends replacing "All cyber systems sharing..." with "All BES Cyber Systems

#	Organization	Yes or No	Question 38 Comment
			sharing..."
38.5	Duke Energy	Agree	The second sentence is a requirement, not part of a definition; consider moving. Specify that "All cyber systems" only applies to BES Cyber Systems. This definition, particularly the concept of "sharing one or more common electronic access points or components" is much more practical in a power plant environment. See previous comments on R11, R12, R13.
38.6	Public Service Enterprise Group companies	Agree	There is general agreement, but need for clarification in the language in one regard. Please clarify whether this requirement would necessitate classifying a Distribution cyber system at a High Impact level if both the Distribution cyber system a High Impact BES cyber system at substation are interconnected using a single router/firewall device to a communications provider. I.e., effectively an additional router/firewall would be required in this situation to not entail classification of the Distribution cyber system at a High Impact level.
38.7	Consultant	Disagree	According to this definition electronic access point where electronic access cannot be controlled for communication paths that transmit and/or receive digital information would not be considered an access point?An access point should defined as locations where information crosses the established protection boundary, or as the locations where external connectivity or remote access occurs. An access point is not dependent on the ability to control the communication path. The sentence "All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s)." is a requirement. It is not a definition nor part of a definition. The concept is sensible, but still not a definition. Suggest moving this to the requirements table.Suggest modifying this definition to be consistent with "External Connectivity" and "Remote Access" definitions.

#	Organization	Yes or No	Question 38 Comment
38.8	Northeast Utilities	Disagree	Agree in principle with the definition but disagree that all cyber assets sharing the access point will be treated at the highest BES Cyber System impact categorization. This will have a big impact on development and test systems as well as other related but not critical systems. How will this impact DMZ systems which by design are not trusted?
38.9	Alliant Energy	Disagree	Alliant Energy agrees with EEI in that it is appropriate to apply protective measures to the literal ingress points (interfaces) on the electronic access points, but not the requirement to apply protective measures to all of the components that connect to said ingress interfaces (to require this creates a house of mirrors.)
38.10	E.ON U.S.	Disagree	CIP-011, R20.1 See previous comments regarding the definition of “external”.CIP-011, R20.1 “Document all communication paths that transmit and/or receive digital information external to each BES Cyber System.” Does this include the WAN if the defined BES Cyber System is inclusive of multiple sites/locations? All equipment and communication paths such as a Sonet ring?CIP-011, R20.3 The term “access control” should be further clarified. Does implementation of firewall rules alone limiting access as defined in R20.2 meet this requirement, or does this require further mechanisms to provide “access control” on an individual user-basis?CIP-011, R20.4, R20.5, R20.6 See previous comments regarding the definition of “external.”CIP-011, R21.1 How might the logical separation called for here be implemented?CIP-011, R21.2 See previous comments regarding the definition of “external.”
38.11	Progress Energy (non-Nuclear)	Disagree	Communication paths may be better defined by including routable protocol and/or ‘external to the BES Cyber System’.Assuming this is the same as external access point it does seem somewhat repetitious.
38.12	American Electric Power	Disagree	Electronic access point for the purpose of this standard is defined as a point where electronic access can be controlled for communication paths that transmit and receive; or only receive digital information. All cyber systems sharing one or more

#	Organization	Yes or No	Question 38 Comment
			common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).Rational: An electronic access point that provides a transmit and receive path or a receive only path to a BES Cyber System provides an access path into the system to be used for possible exploit. By limiting traffic to transmit only communications the risk to the protected BES Cyber System is reduced since an electronic access point is not provided.
38.13	Entergy	Disagree	Entergy suggests adding specific language to the definition that includes “uses routable protocol or is dial-up accessible”
38.14	APPA Task Force	Disagree	In the APPA Task Force comments for Question 37 we proposed changing electronic access point to electronic access control. We do not feel it is necessary to define an electronic access point. We do believe it is necessary for entities to have control of their boundaries. We have proposed using electronic access control in R10, Account Access Control Specifications, in the place of the term Password since we feel there are other methods of controlling access that are equivalent or superior to password protection. We recommend the drafting team use electronic access control rather than defining another High Impact BES Cyber System outside of CIP-010-1.
38.15	Dairyland Power Cooperative	Disagree	In trying to be general, it adds more question as to the intent. Is an access point one a device physically connecting multiple communications paths? What about a terminal server? Is an authentication server or policy managing server an access control point even if it is not in-line with the path?
38.16	Constellation Energy Commodities Group Inc.	Disagree	Is the intent to require use of hardware firewalls? If so, is it possible to state that clearly? If not, what is the intent?
38.17	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's suggestion below:Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact

#	Organization	Yes or No	Question 38 Comment
			categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement fails to recognize that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.18	LCEC	Disagree	Need to clarify the specific access point from an interface perspective. What is meant by the term controlling access? Is this from a network protocol perspective? Is a radio link that extends serial communications considered to be an access point?
38.19	Progress Energy - Nuclear Generation	Disagree	Not all EAPs constitute the highest degree of risk especially is nuclear facilities which are highly secure.
38.20	PacifiCorp	Disagree	PacifiCorp agrees with EEI's suggestion below:Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement fails to recognize that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.Further, PacifiCorp believes the proposed definition is too broad. The preference would be to and should be restricted it to communications supporting routable protocols and or dial-up communication. In 20.2 the standard refers to the use of an access point on routable protocol and or dial-up paths but the definition is currently proposed to be broader. In plant control systems, we have many devices which use an IP routable protocol and an industrial communication control protocol such as fieldbus or profibus in the same device. The new definition would require each of these devices to be defined as an access point.
38.21	American Municipal Power	Disagree	Please provide a little or no impact category

#	Organization	Yes or No	Question 38 Comment
38.22	FirstEnergy Corporation	Disagree	Please provide clarification and examples on definition. Propose changing the second sentence to “All BES cyber systems sharing one or more common electronic access points or components will be logically separated such that each logical system is treated at its own categorization level or, where not separated, electronic access points will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).”
38.23	Dominion Resources Services, Inc.	Disagree	Please see Dominion’s response to Question 13. The interface between systems contained wholly within an access controlled facility should not constitute an electronic access point or be subjected to the Boundary requirements.
38.24	Southern Company	Disagree	R20.5 Is a single or double access attempt on a single access point required to be reviewed?
38.25	San Diego Gas and Electric Co.	Disagree	SDG&E has concerns about the last half of the proposed definition for electronic access points. If two medium or one medium and one low BES Cyber System share an access point, this definition makes the shared access point High impact? Regardless of other controls that may be in place? We feel that this definition is not reasonable.SDG&E suggests the definition of electronic access points should include the words "...between networks." Otherwise, every device on the network becomes an access point.
38.26	BGE	Disagree	Should include wording to clearly define the communication paths that transmit and or receive digital information to a BES Cyber System.
38.27	Allegheny Energy Supply	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security

#	Organization	Yes or No	Question 38 Comment
			requirements.
38.28	Allegheny Power	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.29	EEI	Disagree	Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.30	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The concept of sharing access points must be better defined. Does connectivity to an outside entity at a firewall constitute a shared access point?
38.31	Luminant	Disagree	The definition of access points infers that cyber systems and BES Cyber Systems can share an access point but 20.2 states that BES Cyber systems must be seperated from other devices. re. Cyber systems protected by same firewall but in different zone
38.32	US Bureau of Reclamation	Disagree	The definition proposed is that "ALL cyber system sharing one or more common electronic access point or components..." Components can mean many things and almost all devices share components which have not impact on the BES. It would be better to indicate that "ALL BES cyber systems sharing one or more common

#	Organization	Yes or No	Question 38 Comment
			electronic access point or BES CYBER SYSTEM components...."
38.33	Constellation Energy Control and Dispatch, LLC	Disagree	The definition should clearly establish that the access point is a place where digital information is transmitted or received.
38.34	US Army Corps of Engineers	Disagree	The definition states that an electronic access point is a point where electronic access can be controlled for communication paths that transmit and/or receive digital information. What does "controlled" mean? Would network switches fall under this definition because network switch ports can be electronically controlled with port security?Suggest definition be changed to: An electronic access point is an electronic security point where traffic flowing from different security areas are restricted, controlled, and monitored from entering or leaving a particular security area. This may be restricting traffic from a lower security area (devices external to the BES Cyber System) from entering a higher security area (BES Cyber System.) It may also be restricting sensitive traffic from leaving a higher security area to a lower security area.
38.35	Bonneville Power Administration	Disagree	The first sentence, "Electronic access point for...digital information.", is acceptable, but only because it says what an electronic access point is, not where one has to be located. Second sentence is completely unacceptable, more so than anything else in the standard, for numerous reasons:First, it leads to the equivalent of CIP-007's including every network device within the Electronic Security Perimeter. In retrospect, that inclusion caused additional workload and costs which far exceeded the gain in security. To repeat that error would be totally unacceptable. The requirement should apply only to BES Cyber Systems, and not all cyber systems.Second, it ignores the level of threat posed by the various systems. Just because a cyber system or even a BES Cyber System is behind the same access point as a High impact BES Cyber System does not mean that poses the same risk to the BES, or even any risk at all.Third, it ignores the possibility of nested access point. For instance, consider systems A and B residing within a highly protected network and sharing a single access point. Add system C residing with a less protected network with an access point to the internet. If A and B access the internet through the same

#	Organization	Yes or No	Question 38 Comment
			access point that C uses, then C has to be treated as stringently as the highest impact of A or B.Fourth, applying impact levels based on the highest level of the BES Cyber System is a problematic issue that has been discussed at length. The mere fact that a cyber component exists within a High Impact BES cyber system does not make that specific component a high impact component. There are levels of impact that should be applied within and to the Cyber System. Devices or equipment (Components) within a High impact BES cyber system, may actually have little or no impact on that cyber system regardless of what happens to them. The standard that applies to that device should not necessarily be tied to the Impact rating for the whole BES cyber system.Finally, the second sentence is a statement of a requirement, not a definition. To use an example, assume a Control Center that relies on nested networks, with the outermost controlling external access, and further firewalls controlling access to their nested layers. The outermost firewall would be a common access point, shared by all systems within the Control Center. In that case, all the cyber systems would have to be treated as BES Cyber Systems at the highest impact level of any BES Cyber Systems in the Control Center. Such a treatment ignores the threat a system might or might not pose to the BES. To provide a somewhat absurd but demonstrative limiting case, a minimally functional print server residing in the outermost layer, barely able to accept an IP address, and having no connectivity except Ethernet on one side and a printer interface on the other, would have to be treated the same as an AGC system within the innermost layer controlling thousands of megawatts of generation at sites scattered across multiple states.Recommendation: Delete the second sentence.
38.36	Southern California Edison Company	Disagree	The requirement does not adequately address the technical nuances of virtualization. The central point of virtualization capability can be interpreted as the “shared” access point. At the same time, the centrally located virtualization device may also be interpreted as a BES critical cyber system. In the first case, the controls for the virtualization system will be those afforded to an access point, which may be less stringent than those afforded to a BES critical cyber system. In the second case, where the virtualization device is a BES critical system, on the user end, end user computing devices such as mobile laptops can potentially be considered as BES cyber system

#	Organization	Yes or No	Question 38 Comment
			component, and on the SCADA end, automation devices would be considered as BES cyber system components. Requirement R21 does not make drawing such distinctions clear of subjective interpretation.
38.37	Oncor Electric Delivery LLC	Disagree	The term “public communication paths” should replace “communication paths”. Systems which are isolated from the internet are less susceptible to cyber attacks.
38.38	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
38.39	Xcel Energy	Disagree	We believe the second sentence places an unnecessary burden on lower impact systems if they are unable to communicate with the higher impact system, as is the case with dial-up based systems.
38.40	We Energies	Disagree	We Energies agrees with EEI Suggest removing the requirement: “All cyber systems sharing one or more common electronic access points or components will be treated at the highest BES Cyber System impact categorization level of the BES Cyber Systems sharing the electronic access point(s) or component(s).” from the definition of electronic access point. In addition, the requirement is not clear that a firewall with multiple interfaces has the ability to support multiple electronic security perimeters with differing security requirements.
38.41	US Army Corps of Engineers, Omaha Distirc	Disagree	What does "controlled" mean? Definition also appears to contain a requirement "All cyber systems sharing one or more . . " The requirement doesn't appear to be in line with industry practice. A firewall can protect 2 or more networks from external connections and from each other. Both networks do not have to be at the same sensitivity level. suggest definition be changed to:An electronic access point is an electronic security point where traffic flowing from different security areas are restricted, controlled and monitored from entering or leaving a particular security area. This may be restricting traffic from a lower security area (devices external to the BES Cyber System) from entering a higher security area (BES Cyber System.) It may

#	Organization	Yes or No	Question 38 Comment
			also be restricting sensitive traffic from leaving a higher security area to a lower security area.

39. Tables R20 to R22 provide direction concerning what impact level of BES Cyber Systems to which Requirements R20 to R22 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Many commenters disagreed with the proposed BES Cyber System impact levels and made suggestions to clarify them, including suggestions to revise or refine the impact levels based on the particular characteristics of the BES Cyber Systems involved. In response, the SDT has made changes to include an applicability column in each table for each requirement. The applicability column further refines the set of BES Cyber Systems and assets to which each part of the requirement must be applied. For example, the SDT made changes to the applicability column to include the scoping filter of External Routable Connectivity where the use of a routable connection would be required to comply with the requirement, such as the requirement to have Electronic Access Points.

The intent of this approach is to refine the scope of requirements that apply to each type of BES Cyber System or device based on its characteristics. The drafting team recommends that commenters carefully review the proposed applicability column in the table for each requirement in the CIP Version 5 standards.

#	Organization	Yes or No	Question 39 Comment
39.1	US Army Corps of Engineers		The statement in Table R21, 22.1 "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20.", is confusing. What is the standard trying to say here?
39.2	GE Energy	Agree	20.2: Low BES systems should be required to document and implement access controls.
39.3	Black Hills Corporation	Agree	21.1 requires further definition of logical separation requirements in a disaster recovery scenario. As stated, this does not allow for control centers to back-up each other in a fail-over mode for disaster recovery.
39.4	Duke Energy	Agree	Agree if the external connectivity is via a shared electronic access point as discussed in previous comments.Apply all requirements, where currently in place, only for external connectivity. 20.6: Review of logs every 7 days is not practical.21.2: Only

#	Organization	Yes or No	Question 39 Comment
			require for external connectivity
39.5	Progress Energy (non-Nuclear)	Agree	See comment 14.
39.6	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
39.7	GTC & GSOC	Agree	We recommend a slight rewording of R20.2 as follows “Establish an electronic access point that denies access by default and allows explicitly authorized communication on each path where a routable protocol or dialup communication exists between BES Cyber Systems and other devices.”
39.8	E.ON U.S.	Disagree	: E.ON U.S. does not believe there is a need for compliance requirements for low impact systems. High Impact has such a short timeframe for revocation, that it would require employees be available to revoke privileges 24/7. The SDT should adopt a more reasonable time frame- at least 24 hours. E.ON U.S. believes that R22 is merely a repeat of other requirements and therefore should be deleted
39.9	NextEra Energy Corporate Compliance	Disagree	: NextEra believes it is unclear what the timeframes for Medium Impact and High Impact BEST Cyber Systems are supposed to mean. Do response personnel have to review security logs related to external connectivity every 48 hours or are the expectation for designated personnel supposed to respond to an alert within a 48 hour period? The recommendation is to document and establish one or more processes for automated alerting and response to alerts by designated response personnel for unauthorized access attempts at each electronic access point. This requirement would be applicable to both Medium and High Impact BES Cyber Systems. If automated alerting and notification is not technically feasible, Responsible Entities should be able to develop a process to manually review security logs to determine potential cyber security incidents.

#	Organization	Yes or No	Question 39 Comment
39.10	Regulatory Compliance	Disagree	20.1 STRIKE "Required for Low Impact20.5 Propose - 72 hours for Medium Impact Propose - 48 hours for High Impact21.1 - STRIKE "required" for Medium Impact
39.11	BGE	Disagree	20.5 timeframe should be consistent for medium and high.
39.12	Florida Municipal Power Agency	Disagree	22.2 - Add medium, require low to asses quarterly. Consider high impact to review 'critical' patches within 7 days.22.3 - This should be consistent with R18; medium should be required to monitor their systems. Low should review logs at least quarterly for events, or at least have an automated system in place to alert for specific threats.
39.13	ERCOT ISO	Disagree	22.2-22.3: Should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
39.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
39.15	The Empire District Electric Company	Disagree	Comments: For items 20.4 - 20.6, we believe "for external connectivity only" should be removed from the impact levels to properly coordinate with the comments on these items made under question 37.
39.16	Progress Energy - Nuclear Generation	Disagree	Durations should align with information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
39.17	EEI	Disagree	EEI recommends deleting R21 because it is vague and the risks are addressed in R20. Introducing boundaries within engineered systems will result in decreased reliability.
39.18	Entergy	Disagree	Entergy suggests making R20.3 and R20.4 apply to low impact assets.

#	Organization	Yes or No	Question 39 Comment
39.19	MRO's NERC Standards Review Subcommittee	Disagree	For items 20.4 - 20.6, we believe “for external connectivity only” should be removed from the impact levels to properly coordinate with the comments on these items made under question 37.
39.20	US Army Corps of Engineers, Omaha Distirc	Disagree	Intent of 22.1 is unclear
39.21	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
39.22	Luminant	Disagree	Low impact BES Cyber Systems should be protected but not have to be seperated from all other cyber systems. re introduces the concept of cyber systems in "ESP". R21 How can cyber systems be shared and not be a BES Cyber System
39.23	LADWP	Disagree	Low impact requirements will become an administration issue.
39.24	Minnesota Power	Disagree	Per the discussion regarding these tables in Question 37, Minnesota Power recommends that for Parts 20.1, 20.2, 21.2 and 22.1 “Required” be removed for Low Impact BES Cyber Systems.
39.25	Constellation Energy Commodities Group Inc.	Disagree	Please define the stipulation ‘Required for external connectivity only’. In 20.5, aligning the time requirement on 48 hours for clarity and consistency.
39.26	American Municipal Power	Disagree	Please provide a little or no impact category
39.27	Puget Sound Energy	Disagree	Puget Sound Energy suggests aligning Table 11 with Table 12. Table 13, Table 14, and Table 22. Puget Sound Energy suggests including wording similar to Table 11: “Required for external connectivity only”.
39.28	FirstEnergy Corporation	Disagree	R20 - Timeframes should not be in ‘hours’ (i.e. less than a full day). Tracking by time

#	Organization	Yes or No	Question 39 Comment
			rather than days would not be logistically possible on all systems and compliance could not be maintained.The new requirements now have too many different time frames to meet. Again, not logistically possible on all systems and compliance could not be maintained for larger utilities.R21 - R21.2 - Remove 'Required' for Low Impact Cyber Systems.R22 - Eliminate - see Q37 above.
39.29	Con Edison of New York	Disagree	R20 dialog box; speaks to inheritance of HIGH Impact BES requirements for all cyber systems with shared access points.o Does the inheritance only apply to R20 requirements or does this mean all requirements for these devices would be at the High Impact level?o If all cyber systems regardless of BES use that are within the same boundary require High, this may cause significant manpower or create the need to isolate the true BES systems. The isolation will take significant time to plan and implemento This standard must allow the use of 1 physical firewall, logically separated to isolate networks without inheritance of BES levelR21.1 does this require Cyber Components on the same isolated network be logically separated? Is that correct?o This should not apply to devices on the same network.o Should only be required for high.R20.6 - if automated review and alerting is used this should not be requiredR22 mentions established physical boundaries --- the draft CIP standards do not mention physical boundaries are the PSP requirements defined in this version?
39.30	Southwest Power Pool Regional Entity	Disagree	R20: Distinction between external and non-external connectivity is not appropriate. R22: Patch management should be applicable to all impact categories.
39.31	Hydro One	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifying "external connectivity" since the criteria limits the scope to remote access. Also recommend removing "within the following time period" from 20.5.Recommend that 20.6 be re-worded to be consistent with FERC Order 706 paragraph 526 - "Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs."Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommended removing R21 in the response to

#	Organization	Yes or No	Question 39 Comment
			Question 37.Recommended moving the R22 criteria in the response to Question 37. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.32	ISO New England Inc	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifing “external connectivity” since the criteria limits the scope to remote access. Also recommend removing “within the following time period” from 20.5Recommend that 20.6 be re-worded to be consistent with FERC Order P526 - <<Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs. >>Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days since 18.2 continuous monitoring satisfies the NOPR directive of seven daysRecommended removing R21 in the answer to question 38Recommend moving the R22 criteria in the answer to question 38. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.33	Northeast Power Coordinating Council	Disagree	Recommend that 20.4 and 20.5 should be Required instead of specifying “external connectivity” since the criteria limits the scope to remote access. Also recommend removing “within the following time period” from 20.5.Recommend that 20.6 be re-worded to be consistent with FERC Order 706 paragraph 526 - “Some manual review of logs to improve automated detection settings, even if alerts are employed on the logs.”Recommend that 20.6 High Impact and Medium Impact BES Cyber Systems should be 30 calendar days. Requirement 18.2 continuous monitoring satisfies the NOPR directive of seven days.Recommended removing R21 in the response to Question 37.Recommended moving the R22 criteria in the response to Question 37. The moved 22.2 and 22.3 should apply to Medium Impact BES Cyber Systems as well.
39.34	National Grid	Disagree	Refer to comments in Q. 37.
39.35	Oncor Electric Delivery LLC	Disagree	Requirement 20.6 should provide for a review every 30 days.
39.36	US Bureau of	Disagree	Requirement 22.1 conflicts with earlier requirements regarding controls on remote

#	Organization	Yes or No	Question 39 Comment
	Reclamation		and wireless access.
39.37	San Diego Gas and Electric Co.	Disagree	SDG&E feels that too many classifications make compliance more difficult and likely more risky. We would suggest making the time in R20.5 24 hours for both High and Medium impact systems.SDG&E also feels that instead of using the word “impact” for these Requirements, apply a concept of “risk” for inclusion. We would want to identify the risks with associated systems security and protect accordingly.
39.38	LCEC	Disagree	See previous comments
39.39	Bonneville Power Administration	Disagree	See Question 37, above.
39.40	Constellation Energy Control and Dispatch, LLC	Disagree	See response to question number 37.
39.41	ReliabilityFirst Staff	Disagree	Suggest “30 calendar days for external connectivity only” for Medium Impact in row 20.6. Suggest “Required” for Medium Impact in rows 22.2. and 22.3.
39.42	Ameren	Disagree	Suggest removing R21.2 from Low Impact Systems.
39.43	Alberta Electric System Operator	Disagree	Table R20 - For 20.5 set Low Impact to “120 hours for external connectivity only”; for 20.6, set Medium Impact to “30 calendar days for external connectivity only”Table R22 - Consider making 22.1, 22.2, 22.3, 22.4 Required for all Low, Medium, and High Impact BES Cyber Systems because they are protecting the boundary.
39.44	Consultant	Disagree	The impact levels would be impacted by previous comments on this group of requirements.The terminology "for external connectivity only" is redundant as the access point is where external connectivity occurs. Suggest removing these words from the table where they occur.

#	Organization	Yes or No	Question 39 Comment
39.45	Southern California Edison Company	Disagree	The standard should read such that the centralized/federated primary virtualization system and its back-up are afforded protections commensurate with the impact level of the automation devices that support a particular reliability function. The standard should comply with the intent of Order 706 to prevent intentional or accidental misuse of BES components and limit BES cyber system classification to the automation nodes and virtualization nodes. End-user computing devices in a virtualization system should be classified as conduits to the virtual system that is protected by an electronic border.
39.46	CWLP Electric Transmission, Distribution and Operations Department	Disagree	The time frame for requirement 2.5 would be difficult to comply with for smaller entities.
39.47	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R20 - R22 if our changes proposed in Question 37 are accepted:R20 Table 20.1: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.2: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.3: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.4: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR20 Table 20.5: Low Impact: N/AMedium Impact: 48 hoursHigh Impact: 12 hoursR20 Table 20.6: Low Impact: N/AMedium Impact: N/AHigh Impact: 7 calendar daysR21 Table 21.1: Low Impact: N/AMedium Impact: RequiredHigh Impact: RequiredR21 Table 21.2: (Removed)R22 Table 22.1 - 22.4: (Removed)
39.48	MidAmerican Energy Company	Disagree	While the concept of applying various levels of security controls to BES Cyber Systems based upon their impact level appears to be appealing, until the assessment of each BES Cyber System is made by a utility and the catalog of security controls that must be maintained for each BES Cyber System is understood, the impact level strategy cannot be accessed.

#	Organization	Yes or No	Question 39 Comment
39.49	PacifiCorp	Disagree	While the concept of applying various levels of security controls to BES Cyber Systems based upon their impact level appears to be appealing, until the assessment of each BES Cyber System is made by a utility and the catalog of security controls that must be maintained for each BES Cyber System is understood, the impact level strategy cannot be accessed.

40. The configuration change management requirement is centered on the identification of a component inventory and baseline configuration. Do you agree with the list of criteria that are included in the baseline configuration? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the baseline and managed through the configuration change management process? Do you agree with the list of criteria that are included in Requirements Table R23? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in Table R23? Please explain and provide any suggestions for modification.

Summary Consideration:

Commenters are concerned about a lack of clarity on what is expected for a baseline configuration, and if it should be applicable to an entire BES Cyber System or to individual components. Commenters also expressed a lack of understanding on how detailed inventories should be and to what category they should apply. Many comments addressed the requirements that include component-based actions for low-impact BES Cyber Systems. These are viewed as potentially overwhelming in the overall CIP compliance process. Also, identifying the physical location of a virtual component is identified in several comments as "confusing." Concerns were also identified about the definitions and clarification around terms. For example, what is meant by "Other documentation," "baseline configuration," and "virtual BES Cyber System component" were the primary terms mentioned. Also, more specific information on "security controls" was requested.

This requirement has been moved into a new standard, CIP-010-1 -- Cyber Security — Configuration Management and Vulnerability Assessments. In response to stakeholder comments, the drafting team has provided additional guidance in the 'Application Guidelines' section for the standard regarding the elements of a baseline configuration. The requirement to have an explicit inventory has been removed. This requirement is effectively inferred by the requirement to document a baseline configuration. The drafting team also agrees that maintaining an inventory for all Low Impact BES Cyber Assets within the current compliance framework in which the NERC CIP standards exist is problematic. As such, the drafting team has made an effort to prioritize controls for Low Impact BES Cyber Assets that don't require the documentation of every individual component and may be managed on a site-by-site basis, where feasible.

Several commenters suggested that inventories and monitoring should also apply to Medium and High Impact categories, since impact of the Low category to the BES Cyber System is minimal, and the effort appears to be greater than the benefit. In addition, there are questions on the timeframe and processes for monitoring. Does it need to be real time or can the Responsible Entity establish a tailored schedule for response to the detection of unauthorized changes? With regard to Requirement 23, Part 23.2, several commenters stated that it was written around typical IT equipment configurations and not the multitude of devices within generating or transmission facilities. They believe that because of this situation, the requirement should be limited to control centers similar to Requirement 23, Part 23.6. They further state that for generating facilities and substations, it would be adequate to require the entity to document and implement one or more processes for configuration change management, and that this would be applied to all Low Impact, Medium Impact, and High Impact BES Cyber Systems.

The drafting team intends for the monitoring and alerting capabilities to occur on a near real-time basis. The drafting team appreciates the concerns regarding substation and generation environments and believes that tools to perform these processes on a near real-time basis in these environments are either too immature to be included as part of a mandatory standard or simply do not exist, particularly since a large number of these cyber assets have no external communication method. Additionally, the drafting team believes that other NERC reliability standards, such as those regarding protective relay maintenance and testing, provide some level of mitigation for this lack in currently available technology.

The configuration management requirements state that an inventory must be developed of the physical or virtual BES cyber components "excluding software running on the component". Several commenters questioned why software should not be considered as constituting a "virtual" BES cyber component. Many comments were also submitted on what is perceived as a cumbersome process around inventory, monitoring, and responding to changes in the baseline configuration. They state that the criteria should be simplified, with items such as removing "physical location" from the requirement.

The drafting team has attempted to address these concerns by modifying the impact levels to which they apply. The drafting team, however, continues to believe that a rigorous configuration management program, including documented baseline configurations, is essential to an effective cyber security program.

#	Organization	Yes or No	Question 40 Comment
40.1	USACE - Omaha Anchor		23.2 - clarify "software" - is this all software on the machine or version of the OS?
40.2	US Army Corps of Engineers		Does requirement R23.7 "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes" imply or require automated monitoring?
40.3	WECC		Not sure that baseline is the right word to use as many entities define baselines only at specific times in implementation projects or as part of system hardening. Item 23.5 says to "assess potentially impacted security controls" then Item 23.6 says to test them. Is this the same requirement? The second bullet in 23.6 is very difficult to read. Consider having a separate requirement for 1) Change Management Criteria, 2) Testing Criteria, 3) Test Environment Criteria.Virtualization is mentioned in 23.1. This is good, but should probably be considered in other requirements as well. In 23.2 an inventory is required of components. Based on the current definition of component,

#	Organization	Yes or No	Question 40 Comment
			this would not need to be done down to the device level; however, management at the device level is needed for effective application of change management.In 23.6 there does not appear to be a provision for changes to the baseline configuration itself. Also, the requirement for established procedures was removed. This will lead to inconsistent testing and makes auditing much more difficult.
40.4	Exelon Corporation	Agree	Exelon seeks clarification on the following questions. Do Requirements 23.2 and 23.4 include relay and SCADA equipment settings and settings changes? Would documentation of an assessment be required in a test environment before each and every relay or SCADA setting change?
40.5	Florida Municipal Power Agency	Agree	FMPA agrees with the intent of the requirements but believes significant improvements can be made.There is no process to identify when any changes made to the BES might affect the actual identification of the BES component(s) as a new impact rating.FMPA does not believe that a Responsible Entity will be able to fully comply with some of these standards as they are written. For example, to fully assess how a change might impact the BES Cyber System could be interpreted to mean the RE would need a fully functional replicated copy of the production environment. FMPA does not believe this is reasonable.
40.6	Progress Energy - Nuclear Generation	Agree	R23 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
40.7	CWLP Electric Transmission, Distribution and Operations Department	Agree	R23.5. What are the ramifications to the Responsible Entity if the assessment is inaccurate and a change does adversely affect the BES Cyber System? Conducting an assessment does not guarantee success as there are always unforeseen incidents that may impact upgrades and new installations.
40.8	Xcel Energy	Agree	We believe additional guidance is requires as to what type of monitoring is expected

#	Organization	Yes or No	Question 40 Comment
			in R23.7. Is active monitoring expected, or periodic review of logs sufficient?
40.9	Dairyland Power Cooperative	Disagree	23 Note that on many SCADA systems, the simple matter of summing two telemetered values may require the modification of software/scripts. For simple calculations such as these the overhead of change control and security track will serious slow the process of making adjustments during a field checkout. Are there any further criteria that can be used to minimize the overhead on changes that are not reasonably expected to impact security posture?
40.10	FirstEnergy Corporation	Disagree	23.1 - Should also exclude data.23.2 - Cyber System Components is used two different ways in 23.1 and in 23.2. And neither uses really match the definition provided in CIP 010. What is expected for a baseline configuration for an entire BES Cyber System as opposed to a configuration for an individual component?23.3 - Change 30 days to 90 days. Remove 'other documentation as necessary' or be more specific as to what that means.23.2 - 23.4: Is the standard requiring the Responsible Entity to update the baseline documentation every time a patch is applied?
40.11	Dominion Resources Services, Inc.	Disagree	23.1 & 2 & 3(inventory only). It should be clarified that the inventory is for in-service equipment and that location refers to an area or room and not to a rack or slot. 23.4. A definition of "Authorize" should be provided.23.5. At the May workshop, an entity said they were audited by 2 regions and each region had a different definition of what cyber security controls were. On this point Dominion recommends that the word "Assess" be changed to "Define cyber security controls and assess." 23.7 Dominion is unclear how this requirement can be met. For example, an alarm is received when a relay is placed into "configure" mode, but there is no ability to see what is being changed. Stated differently, Dominion can respond to a change, but cannot monitor what is being changed. If the relay is in a remote location, Dominion's response time will be impeded. This is the best case scenario. Much equipment does not alarm when its configuration has been changed (e.g., a computer does not generate an alarm when a new program is loaded.) Dominion requests that this requirement be

#	Organization	Yes or No	Question 40 Comment
			removed.
40.12	BGE	Disagree	23.2 custom software/scripts should not be part of the baseline inventory. Recommend having 1 inventory for Low, medium and High.
40.13	American Electric Power	Disagree	23.3: Regarding "Authorize and document changes to the BES Cyber System that deviate from the existing inventory and update the inventory and other documentation as necessary within 30 days of the change being completed", what changes must be authorized and documented? Is this targeting physical network changes or adding/deleting equipment? Is this targeting software changes?23.7: Regarding "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes", is this a continuous monitoring requirement? If not, what is the frequency that a comparison between the actual and latest approved baseline be conducted? Comparing baseline to existing configurations would be a manual process is most instances. Suggest rewording to specify that this will be conducted on the individual BES Cyber System components at some frequency, possibly quarterly.
40.14	Regulatory Compliance	Disagree	23.4 - propose adding - "Authorize and document changes that present a high risk to the BES....23.4a - additional criteria - Entity documents changes into categories of risk, based on the risk assessments determines if changes are in or out of scope.23.7 - unreasonable expectation based on the definition of baseline configuration. Instead propose the following: Do an annual review, recapturing the baseline configuration. Review for unauthorized changes during this process. If unauthorized changes are found remediate and document within 60 days of the documented annual review.
40.15	Southwest Power Pool Regional Entity	Disagree	23.5: Clarify what is meant by “deviation from the existing baseline configuration.” A new or replacement BES Cyber System Component needs to be validated before placing into service even if it uses an existing baseline configuration if for no other reason than to verify the configuration as built matches the baseline. Additionally, “potentially impacted cyber security controls” is highly subjective and open to

#	Organization	Yes or No	Question 40 Comment
			interpretation. Remove the "potentially impacted" language. 23.6: "included in the baseline configuration of the BES Cyber System" has a vendor baseline connotation. Consider clarifying to refer to the currently approved configuration of the production BES Cyber System. Additionally, the criteria need to clarify just what is meant by "baseline configuration." Does this mean the currently approved hardware and software, including versions or release levels? Or is it less granular, such as "a server running Linux and EMS/SCADA software." Without the clarification, the term is open to interpretation and the ability to audit will be affected.
40.16	MidAmerican Energy Company	Disagree	23.7 Most entities do not have the capability, resources or tools currently to live monitor configuration changes on all category A devices. There could be impacts to performance to run agents on equipment and some vendor supported devices may not allow live monitoring.
40.17	BCTC	Disagree	Â R23. Define in more explicit terms the definition of a "baseline configuration" - what comprises a baseline config - i.e. patch level, etc. R23.6. There are expected to be scenarios whereby a test environment may not exist for a high impact BES Cyber System. In such cases would a scenario like rolling out changes to a non-critical environment represent a test environment from a compliance perspective?
40.18	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. With 100's of low impact BES substations, there are 1000's of BES Cyber System components. These substation devices are being changed daily. The documentation requirements of R23 are overly burdensome with little benefit for low impact BES Cyber Systems. We recommend removing Low Impact BES Cyber Systems from all R23 controls.
40.19	E.ON U.S.	Disagree	CIP-011, R23.1 The requirement states that an inventory must be developed of physical or virtual BES CSC's excluding software running on the component. What

#	Organization	Yes or No	Question 40 Comment
			constitutes a "virtual" BES CSC if not software?
40.20	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
40.21	Constellation Energy Commodities Group Inc.	Disagree	Clarify R23 to not require tracking of routine changes within the container of existing software (example, add a point or change data type of a point), but to track code migrations and changes to the baseline of deployed components.
40.22	The Empire District Electric Company	Disagree	Comments: This requirement, especially evident in item 23.2, appears to be written around typical IT equipment, and not the multitude of electronic programmable devices an entity will encounter in the field at a generating facility or substation. Therefore, we believe the current intent of this requirement should only apply to control centers, similar to item 23.6, where typical IT equipment is becoming more of the standard.For generating facilities and substations, we believe it would be adequate to require the entity to document and implement one or more processes for configuration change management, and this would be applied to all Low Impact, Medium Impact, and High Impact systems.
40.23	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy disagrees with the list of criteria in the baseline configuration. Maintenance of such a list including, software versions, active ports and services, any patches and custom software/scripts will be burdensome and subject to unintended error as the list will contain a significant number of entries. CenterPoint Energy is unsure of the value of such a list regardless of R23 assertion that it is meant "...to prevent and detect unauthorized modifications to BES Cyber Systems." Unless such a list is reviewed on a daily basis, or perhaps even more often, there is no "detection" involved. As to "protection", CenterPoint Energy fails to see where that would occur from the development of and maintenance of such a list. CenterPoint Energy does understand the need to maintain current configuration data, however this criteria is too prescriptive.

#	Organization	Yes or No	Question 40 Comment
40.24	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Disagree	Having a hard time with the idea of documenting the physical location of the cell phone described in question 1.a, and with documenting every change in its location within 30 days of every move.
40.25	Progress Energy (non-Nuclear)	Disagree	If the BES Cyber System Component is a microprocessor relay/device, this can get complicated. These devices have numerous 'configurations' based on an application. Also, firmware versions would need to be considered. Today, most utilities lock firmware on many relay models. Another issue may be when a cyber component is returned to a manufacturer for repair - how do we verify that a replaced operating system component is compliant.R23.2 need to be explicit that the baseline is the inventory in existence at compliance time for existing systems.R23.7 in most existing generating plant systems would not be able to meet this requirement and the value is questionable since the use of administrator accounts is highly restricted by multiple other requirements.CIP-011 - R23 - Need clarification as to what constitutes a "virtual BES Cyber System Component".
40.26	Midwest ISO	Disagree	It is not clear how R23 inventories differ from those inventories that must be identified in CIP-010 R2. To the extent that these are duplicate, the duplications should be eliminated.
40.27	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
40.28	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R23, but recommends changes as follows: o For Parts 23.1 and 23.2, Minnesota Power recommends that Standards Drafting team define what constitutes a "Virtual BES Cyber System Component." o Regarding Part 23.2, Minnesota Power recommends that the Standards Drafting Team further define the level of software versions are required for tracking purposes. For example, an EMS has hundreds of small programs that make up the system. Each of these individual programs is combined under an

#	Organization	Yes or No	Question 40 Comment
			overall version number. In addition, different Registered Entities, with the same EMS version, may have different internal applications with different levels of fixes. To what level should those be documented? o For Parts 23.5 and 23.6, Minnesota Power recommends that the Standards Drafting Team define the term “cyber security control.” o For Part 23.6, what constitutes a “deviation?” What level of baseline is required? o Regarding Part 23.7, Minnesota Power requests that the Standards Drafting Team consider defining the term “monitor” and identify the level of detail required for these changes. For example many EMS sub-programs constantly create/modify/remove files as a normal course of business. Would these changes need to constantly be reviewed and verified?In general, Minnesota Power believes that the list of items to be tracked/tested/monitored is vague and could cause Registered Entities to incorrectly implement processes to satisfy this Requirement.
40.29	NextEra Energy Corporate Compliance	Disagree	Nextera believes there is not an agreement for the list of criteria that should be included in the baseline configuration, the requirement is a big undertaken to manage the software on BES Cyber Systems and provides little improvement to the reliability of the BES Cyber Systems.The following is the recommended updates:23.2 - Develop a baseline configuration of the BES Cyber System, which shall include an inventory of its physical or virtual BES Cyber System Components (excluding software running on the component), physical location, active ports and services, any patches, and any custom software/scripts.Keeping inventory on running software on medium and high impact BES systems will be a big undertaken. With the other levels of controls to develop baseline configurations, software should be excluded.In 23.7, this implies implementation of automated tools to detect configuration changes. Not all systems will support these tools. If not possible to automate, are manual processes acceptable? If so, wording should specify "automatic or manual detection".
40.30	LCEC	Disagree	No. The baseline configuration is not specific enough and leaves much open to interpretation.

#	Organization	Yes or No	Question 40 Comment
40.31	National Grid	Disagree	o National Grid suggests rewording 23.5 - "Assess changes to baseline configuration to verify controls are not adversely affected ..." o 23.6 - Need more information on testing requirements. o23.7 - Expand on "monitor changes". Is the SDT considering a timeline to respond to detection of any unauthorized changes o National Grid recommends the SDT to check the new EOP Backup Facility Standard for testing in 23.6
40.32	PacifiCorp	Disagree	PacifiCorp seeks clarity on 23.2 as to the 'components'. In the case of a server, is this every component in the case (including fans?) or additionally all apparatus which are directly attached (Mouse, Keyboard etc) which would not normally be included in a change record.
40.33	RRI Energy	Disagree	Part 1: does "active ports and services" refer to the network accessible ports and services as mentioned in the above requirement 17.1?Part 2: Some application uses port ranges. Netstat command only reports actively listening port(s). The requirement explicitly states "active ports and services". Some ports in the port ranges may not be active when the netstat command runs. So when the inactive ports are not in use, depending on the vendor/program, entity could be out of compliance. Active could be replaced with "Active or documented system design ports and services".What does "closely models" mean?Is a "test environment" an actual thing or a state? Example: a generation unit is online generating x MWs - no test environment "state' exists due to the unit being online; a generation unit is in a 2 week maintenance outage, all cyber assets related to the unit are in a test environment "state".
40.34	Northeast Utilities	Disagree	Please clarify 23.7. Specifically, does this monitoring need to be automated? If not, how often will the monitoring need to be performed to meet the standard?
40.35	Network & Security Technologies Inc	Disagree	R23 - Sound configuration change management practices can minimize the risk of unauthorized modifications but cannot "prevent and detect" in all instances. Suggest

#	Organization	Yes or No	Question 40 Comment
			revising the overall goal here.23.6 - Suggest adding a provision allowing a Responsible Entity to suspend this requirement under emergency conditions (e.g., to apply an emergency hot fix needed to restore a disabled or impaired BES Cyber System).23.7 - Absent the use of automated tools, this may be a very hard requirement for Responsible Entities to meet. Suggest SDT consider reasonable approaches to how it might be done on a manual basis (e.g., periodic comparisons of running configurations and stored configuration profiles) without imposing an undue burden on Responsible Entities with large numbers of High Impact systems and no current investment in automated monitoring.
40.36	Consultant	Disagree	R23. The terminology "incorporate the criteria" seems incorrect. The table is actually listing the requirements. Suggest changing to "incorporate the requirements".Table R23 - Item 23.1 The terminology "virtual BES Cyber System Components (excluding software running on the component)" seems confusing. Software would seem to be the 'virtual' component, so if software is excluded then the 'virtual' aspect seems unnecessary. Please clarify the intent of this requirement. Item 23.1 The "physical location" of a "virtual component" does not appear to make sense. Suggest rewording to specify physical location of hardware. Item 23.1 & 23.2 Qualification of "physical or virtual" components should be unnecessary. The defined term 'BES Cyber System Component' should be the basis for the requirement. Adding these qualifiers implies that the definition is not adequate. Suggest removing the qualifiers physical or virtual.Item 23.2 Suggest changing "software (including version)" "installed software versions".Item 23.2 & 23.6 The terminology "any patches, and any custom software/scripts" is vague. Suggest changing to "installed patches, and installed custom software or custom scripts".Items 23.3, 23.4, & 23.6 - Suggest changing "that deviate from the existing" to "that modify the existing".Item 23.4 - The terminology "and other documentation" is vague and subjective. Suggest deleting that phrase from this item. While "other documentation" may require an update this requirement should stay focused on configuration status.Items 23.3, 23.4, & 23.5 - The terminology shifts from 'BES Cyber System Components' used in Items 23.1 & 23.2 to 'BES Cyber System' in the last three items. If the inventory & baseline configuration is on the

#	Organization	Yes or No	Question 40 Comment
			component level then these three items should address changes on the component level to be dealing at the same level of detail. Suggest using consistent terminology in this table, either 'systems' or 'components'.Item 23.6 - Suggest deleting "each" as an unnecessary word. "For changes that modify the..." is better phrasing.Item 23.6 - Suggest deleting "software versions, active ports and services, any patches, and any custom software/scripts included in the" as unnecessary wording. The statement that the test environment closely models the baseline configuration should be adequate.Item 23.6 - Suggest punctuation or reformatting the second bullet for clarity. Possibly a separate line item: "For testing changes that modify the document: (1) the results of the testing (2) the difference between the test environment and the baseline configuration..., and (3) a description of measures used to account for the differences in operation between the test environment and the baseline configuration...."Item 23.7. This requirement statement is vague. Does it mean an inventory of hardware to monitor if any additional hardware was added, or hardware was removed? It appears to relate to some type of software status monitoring, but is not clearly stated. The terminology "respond to the detection of any unauthorized changes" is not clear and is subjective. As it is written, suggest deleting this item, or clarify the wording so it is a viable requirement.
40.37	ISO New England Inc	Disagree	r23.2 - custom software/scripts? Maybe better language is those custom software scripts that are required for the function of the BES cyber system component would be more appropriate. Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see answer to question 41)R23.5 A entity may define that it's only security control is password complexity while other may try to adopt a Security Controls from the Center for Internet Security. As an entity defines more security controls the higher the risk for violating a requirement. Can cyber security controls be defined or identify requirements within this standard?R23.5 looks like the wording of the requirement allows the change to be made to production then test (after the change is made) to determine if the security has been adversely affected? Appears to contradict R23.6.As written, 23.5 is confusing. Suggest using “Assess changes to baseline configuration to verify controls are not adversely affected

#	Organization	Yes or No	Question 40 Comment
			..."Recommend the SDT check the new EOP Backup Facility Standard for testing in 23.6R23.7 What is the timeframe for monitoring? R23.4 gives 30 days to document the difference so can you monitor 30 days after the change. Does monitoring need to be real-time or can a daily process be used (other than weekends and holidays) to detect changes and reconcile to change management requests?
40.38	Independent Electricity System Operator	Disagree	R23.2 - what is meant by "software". Is this requiring that the version of Notepad, Wordpad, WinZip be recorded or only software that is needed to operate the component?- R23.5 A entity may define that it's only security control is password complexity while other may try to adopt a Security Controls from the Center for Internet Security. As an entity defines more security controls the higher the risk for violating a requirement. Can cyber security controls be defined or identify requirements within this standard?- - R23.5 looks like the wording of the requirement allows the change to be made to production then test (after the change is made) to determine if the security has been adversely affected? Appears to contradict R23.6.- - R23.7 What is the timeframe for monitoring? R23.4 gives 30 days to document the difference so can you monitor 30 days after the change. Does monitoring need to be real-time or can a daily process be used (other than weekends and holidays) to detect changes and reconcile to change management requests?- R23.3: replace "existing inventory" with "existing baseline" since above the baseline configuration was defined to include an inventory...; replace "update the inventory" with "update the baseline"- R23.3: what is "other documentation"- R23.3: is 30 days calendar days or business days?- Not clear on the difference between 23.3 and 23.4- R23.5: define "cyber security controls"- R23.6: could the statement "test the changes to the BES Cyber System in a test environment..." be changed to replace the second "test" with another word-what if it is tested in an environment that is not "test" but meets the requirements as stated?
40.39	Ameren	Disagree	R23.3 - Does change only constitute replacing hardware as inventory and replacement of software is not a requirement for low systems? Need to clarify requirement.R23.4 - This requirement will be challenging to audit as there is no clear lower threshold for

#	Organization	Yes or No	Question 40 Comment
			changes to the baseline configuration. Suggest adding the term significant changes.R23.7 - Is this requiring the installation of additional software to perform this function? Some systems may not allow the addition of this type of software, this requirement will likely end up needing a TFE.
40.40	Allegheny Energy Supply	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.
40.41	Allegheny Power	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.
40.42	EEI	Disagree	R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high

#	Organization	Yes or No	Question 40 Comment
			impact cyber systems.
40.43	Constellation Power Source Generation	Disagree	R23.7 describes monitoring, but not how the monitoring should be implemented (automated, manual, etc). What is the timeline to respond to the detection of unauthorized changes? Yearly? Daily? Continuously? A suggestion would be a yearly manual monitoring system.
40.44	Hydro One	Disagree	Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see response to Question 41).As written, 23.5 is confusing. Suggest rewording to “Assess changes to baseline configuration to verify controls are not adversely affected ...”Recommend the SDT check the new EOP Backup Facility Standard as it applies to testing in 23.6.Please explain the rational to limit 23.6 to Control Centers only.
40.45	Northeast Power Coordinating Council	Disagree	Recommend that 23.2 should remove physical location since it is covered in the updated 23.1 (see response to Question 41).As written, 23.5 is confusing. Suggest rewording to “Assess changes to baseline configuration to verify controls are not adversely affected ...”Recommend the SDT check the new EOP Backup Facility Standard as it applies to testing in 23.6.
40.46	Garland Power and Light	Disagree	Requirement 23.2 23.4, 23.6 and 23.7 - should not apply to database changes or display changes
40.47	Alliant Energy	Disagree	Requirement 23.7 forces entities to implement discovery tools where they may not already exist into environments that may incur negative impact from the very nature of these discovery mechanisms. Where the operational risk of discovery tool deployment precludes its introduction, this requirement would necessitate manual processes. These manual processes would tax the operational resources normally dedicated to increasing the reliability of the BES.
40.48	Public Service Enterprise	Disagree	Requirement 23.7 may not be technically feasible for certain types of BES Cyber

#	Organization	Yes or No	Question 40 Comment
	Group companies		System Components such as older generation or legacy Remote Terminal Unit (RTU) products. To implement this requirement, an Operating System level change to the component may be required, which may be infeasible or not available from the Original Equipment Manufacturer (OEM). This requirement needs to be qualified with the phrase “where technically feasible”.
40.49	San Diego Gas and Electric Co.	Disagree	SDG&E feels that unless there is a major change in the number of types of assets that fall into the low category, there is little reason to have these assets be subject to a different set of requirements than those in the medium and high impact areas. Also, if there is consistency in the application of medium and high impact assets for R23.2 and R23.4, then why is R23.5 only required for high impact assets? SDG&E also requests an example of a virtual BES Cyber System Component (excluding software running on the component).
40.50	Duke Energy	Disagree	Some software on a BES Cyber system may not be relevant to the system (ex. Microsoft calculator or other bundled software) we don’t want to include a version of that. Suggest removing software since the software itself may be the BES cyber systemRequirements 23.3, 23.4, 23.5 - authorization should be able to be made more than 30 days BEFORE the installation.Requirements 23.3, 23.4: documentation via "red-marked" drawings ("interim as built") should satisfy this requirement. Is that the case?Requirement 23.5: as written, it allows the assessment to occur AFTER the fact. Should this not occur BEFORE the change is made?Requirement 23.6: with the proposed definition, it is open for interpretation how closely test environment should model the production environment.Requirement 23.7: what is the expectation for implementing this control? Manual? Automatic? Suggest removing. We are unaware of any device capable of doing this.
40.51	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments to require the current drafted language of R23 Table 23.1 - 23.7 for Control Centers Only. We also offer the following recommendation to cover a Configuration Change Management process for the rest of the facilities:R23 Table 23.8 (NEW): Develop one or more processes for

#	Organization	Yes or No	Question 40 Comment
			configuration change management for BES Cyber System Components in generation and transmission facilities.R23 Table 23.8: Low Impact: RequiredMedium Impact: RequiredHigh Impact: RequiredR23. Objective:To prevent and detect unauthorized modifications to BES Cyber Systems. R23. Requirement:Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R23 - Configuration Change Management.
40.52	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent and detect unauthorized modifications to BES Cyber Systems") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.In addition, Section 23.7 of Table R23 has issues.It is not clear what is meant by "monitor changes...." If this implies some form or ongoing or periodic "monitoring" consider the following:Depending upon the definition of "change" and because of the nature of devices located at substations and other BES equipment, any form of ongoing check or monitoring would be extremely difficult. Because there is the potential for each device to have specific configurations and settings depending up the conditions of the circuit it might be connected to, this would mean that each piece of equipment would have to be manually connected to and checked on a periodic basis. These are industrial controls that are not normally connected to unless service is required for some reason. The definition of a change should not include day to day work processes that are performed to keep the lights on such as settings changes, resetting relays, AV signature updates, or other services and settings kinds of activities. Nor should it necessarily include data changes that do not affect the executable code or configuration of the system. We would expect to be able to define what a change is within our environment.Recommendation: Delete 23.7. Modify R23 to read:Objective 23 - To prevent and detect unauthorized modifications to BES Cyber Systems.R23. Each Responsible Entity shall document and implement processes that incorporate the criteria in CIP-011-1 Table R23 - Configuration Change Management. Such processes shall include an Entity-specific

#	Organization	Yes or No	Question 40 Comment
			definition of what constitutes a system change.
40.53	US Bureau of Reclamation	Disagree	The table requires additional clarification, particularly for different sorts of devices (relays, etc.)
40.54	Con Edison of New York	Disagree	These systems are constantly be upgraded all year long with little impact on any security. The need to do this within 30 days is excessive and should be limited to an annual review.
40.55	MRO's NERC Standards Review Subcommittee	Disagree	This requirement, especially evident in item 23.2, appears to be written around typical IT equipment, and not the multitude of electronic programmable devices an entity will encounter in the field at a generating facility or substation. Therefore, we believe the current intent of this requirement should only apply to control centers, similar to item 23.6, where typical IT equipment is becoming more of the standard.For generating facilities and substations, we believe it would be adequate to require the entity to document and implement one or more processes for configuration change management, and this would be applied to all Low Impact, Medium Impact, and High Impact systems.
40.56	Western Area Power Administration	Disagree	This requires a near-identical test system and makes no adjustments for risk analysis, and does not allow testing on failover devices (maybe) as it says "test environment" specifically. Is that truly the intent?
40.57	We Energies	Disagree	We Energies agrees with EEI: R23.3Implement and document a process to authorize and document changes to the BES Cyber System and update the inventory and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.We Energies agrees with EEI: R23.4Implement and document a process to authorize and document changes to the BES Cyber System and update the baseline configuration and other documentation as necessary within 90 days for low impact cyber systems, 60 days for medium impact cyber systems, and 30 days for high impact cyber systems.

#	Organization	Yes or No	Question 40 Comment
40.58	Manitoba Hydro	Disagree	We support the baseline approach to change management. It is unclear as to what "other documentation" in Requirements R23.3 and R23.4 is being referenced.
40.59	Emerson Process Management	Disagree	What is the significance of excluding software from the inventory requirement in 23.1 for low-impact BES Cyber System? Cyber security is mostly related to software than hardware. This exclusion does not give any value to the low impact systems.

41. Table R23 provide direction concerning what impact level of BES Cyber Systems to which Requirement R23 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Configuration Change Management" is now addressed in CIP–010–1 — Cyber Security — Configuration Change Management

Commenters raised concerns about requirements that include component level actions for Low Impact BES Cyber Systems, such as inventories and development and maintenance of documentation. Commenters believed that the effort needed to implement those actions will detract from other, more critical actions on Medium and High Impact BES Cyber Systems and Components. Some recommendations are to remove Low Impact BES Cyber Systems from all Requirement R23 controls. In addition, because inventories are required in R23.1-2 for Low Impact components, commenters recommend that these should be limited to devices that have an external accessible connection with a potential direct impact on BES reliability. The drafting team appreciates the concern regarding the level of effort necessary for compliance on Low Impact assets. As such, the drafting team has attempted to implement a framework where the controls for Low Impact assets are those that can be implemented at a higher level of abstraction (such as on a site-by-site basis versus a component level basis) or are primarily programmatic or organizational in nature.

Commenters recommended that monitoring changes to the baseline configuration and responding to the detection of any unauthorized changes be limited to control centers only. The commenters submit that although the requirement may be appropriate for certain types of assets, the technology required to monitor many devices in generation and transmission facilities does not exist. As indicated in its response to Question 40, the drafting team appreciates these concerns and has modified the applicability for configuration monitoring to High Impact control centers.

Commenters noted that Requirement R23.2 adds a requirement for a detailed level of inventory including software versions. Commenters were not clear on the granularity required of this inventory. In addition they question how custom code is tracked for systems such as EMS and scripts that are routinely developed to streamline operational functions. In response, the specific language of the requirement regarding the necessary elements in a baseline configuration has been updated by the drafting team with the intent to provide additional clarity. (See Requirement R1, Part 1.1 in CIP-010-5)

Comments were submitted that recommend one inventory be required to cover all Low, Medium and High Impact BES Cyber Systems. It was also suggested that in Requirement R23.6, the requirements identified for Control Centers should only be extended to High Impact BES Cyber Systems as well as Control Centers. In response, the drafting team has adjusted the impact levels of the items that require an inventory to more suitably focus the effort of the Responsible Entity on items that are not as documentation-centric. None of the requirements in proposed CIP-010-5 apply to Low Impact BES Cyber Systems.

Regarding the testing of changes, commenters recommended testing of all High and Medium Impact BES Cyber Systems, not just those in Control Centers. They also recommended, however, that developing a test environment that models the production environment and documents differences should be applied only to High Impact BES Cyber Systems in Control Centers. In response, the drafting team has modified the standard to require testing of security controls for both High and Medium Impact BES Cyber Systems, but only requires testing in a test environment for those High Impact BES Cyber Systems in Control Centers. (See Requirement R3, Part 3.2 in the proposed CIP-010-5).

#	Organization	Yes or No	Question 41 Comment
41.1	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
41.2	Reliability & Compliance Group	Agree	You need to provide a definition of a virtual BES cyber system component.
41.3	LCEC	Disagree	23 What level does the software inventory include? Driver versions? What about devices with embedded OSes? Needs to include functionality testing.Is the requirement in 23.6 for control center only in reference to the cyber system components?
41.4	Black Hills Corporation	Disagree	23.5 should apply to Medium impact BES cyber systems.
41.5	ERCOT ISO	Disagree	23.5-23.7: Should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
41.6	Regulatory Compliance	Disagree	23.7 - High Impact - "required for Control Center only"
41.7	US Bureau of Reclamation	Disagree	All impact levels should have some minimum level of requirement established.
41.8	Southwest Power Pool Regional Entity	Disagree	Although the language will work as written, it could be improved by separating the component inventory requirement defined in 23.1 from the more comprehensive

#	Organization	Yes or No	Question 41 Comment
			requirements in 23.2, making 23.1 applicable to all impact categories. Similar improvement is possible with 23.3 and 23.4. 23.6: Testing prior to implementation should apply to Medium category systems.
41.9	Southern Company	Disagree	As long as there are requirements which include per-component action for each low-impact BES Cyber System, the effort needed to implement those actions will overwhelm the rest of the CIP compliance effort. With 100's of low impact BES substations, there are 1000's of BES Cyber System components. These substation devices are being changed daily. The documentation requirements of R23 are overly burdensome with little benefit for low impact BES Cyber Systems. We recommend removing Low Impact BES Cyber Systems from all R23 controls. R23.1-2 requires an inventory of all Low Impact components, this is an intensive work load addition for the Low category components. Components as identified in the definition include all programmable devices. This includes most instrumentation in a generation unit. This should be limited to devices which have an external accessible connection with a potential direct impact on BES reliability.
41.10	WECC	Disagree	Change management and testing should be done for all medium and high impact level BES Cyber System Components not just control center or high.Criteria should apply to all impact levels.
41.11	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
41.12	The Empire District Electric Company	Disagree	Comments: See comments under question 40.
41.13	US Army Corps of Engineers, Omaha Distirc	Disagree	Define "changes" as used in 23.4. Does requirement R23.7 "Monitor changes to the baseline configuration and respond to the detection of any unauthorized changes" imply or require automated monitoring? If automated monitoring is required this could result in numerous TFE's for other than general processing equipment.

#	Organization	Yes or No	Question 41 Comment
41.14	Alberta Electric System Operator	Disagree	In 23.5 and 23.7, consider setting Medium Impact both to Required
41.15	Entergy	Disagree	Inventory and component baseline configuration management are basic care and feeding requirements generally accepted as best practice - 'systems management 101'; and should therefore apply for intelligent infrastructure employed throughout a control system. It is also clear from Order 706 that this is what FERC intends.
41.16	Consultant	Disagree	Item 23.6 - Stating that this is required for Control Centers only adds an additional dimension to the impact categorization. The impact categorization criteria should clearly identify the assets that go into a particular impact classification. The table should only state whether the requirement is required for that classification or not, it should not add an additional classification criteria.
41.17	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
41.18	Oncor Electric Delivery LLC	Disagree	Need an inventory for Medium and High systems(R23.1) and should document changes for Medium and High systems(R23.3) Requirement R23.7 should allow for manual processes to detect changes. It is also unclear how an entity would document a phased implementation - is it based on "in-service" designation?
41.19	Con Edison of New York	Disagree	o R23 changes and adds to Change Management Configuration requirements. This requirement mentions the need for an inventory of BES cyber components. This is not mentioned in CIP-010 o R23.2 This requirement adds a much more detailed level of inventory including software versions. This would be an extensive task, and does this require an inventory of all, such as any Microsoft Office on the workstations, non- MS app's etc? Shouldn't this be limited to knowing the release level you are on, without the line-by-line level information? How do you handle custom code for custom systems such as EMS?How do you manage scripts, they can be written to pull information from the database as shorthand; would that count? These are routinely

#	Organization	Yes or No	Question 41 Comment
			written by staff to get something quickly, and to address repetitive solutions/commands.
41.20	American Municipal Power	Disagree	Please provide a little or no impact category
41.21	Madison Gas and Electric Company	Disagree	R23.1 states: Develop an inventory of its physical or virtual BES Cyber System Components (excluding software running on the component), including its physical location.The BES Cyber System Component definition states: One or more programmable electronic devices (including hardware, software and data).... This requirement excludes software, but what about data?
41.22	BGE	Disagree	Recommend having 1 inventory for Low, medium and High.
41.23	Hydro One	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber Systems.Recommend 23.6 High Impact BES Cyber Systems should be Required, not Required for Control Center Only.Recommend a clarification of “monitor” in 23.7.
41.24	ISO New England Inc	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber SystemsRecommend 23.6 High Impact BES Cyber Systems should not be Requireed for Control Center Only
41.25	Northeast Power Coordinating Council	Disagree	Recommend that 23.1 and 23.3 should be Required for High Impact, Medium Impact and Low Impact BES Cyber Systems.Recommend 23.6 High Impact BES Cyber Systems should be Required, not Required for Control Center Only.Recommend a clarification of “monitor” in 23.7.
41.26	National Grid	Disagree	Refer to comments in Q. 40.
41.27	San Diego Gas and Electric	Disagree	SDG&E feels that unless there is a major change in the number of types of assets that

#	Organization	Yes or No	Question 41 Comment
	Co.		fall into the low category, there is little reason to have these assets be subject to a different set of requirements than those in the medium and high impact areas. Also, if there is consistency in the application of medium and high impact assets for R23.2 and R23.4, then why is R23.5 only required for high impact assets?
41.28	American Electric Power	Disagree	See comments under question 40.
41.29	MRO's NERC Standards Review Subcommittee	Disagree	See comments under question 40.
41.30	Southern California Edison Company	Disagree	Should be unilateral across all levels.
41.31	ReliabilityFirst Staff	Disagree	Suggest “Required” for Medium Impact in rows 23.5, 23.6, and 23.7.
41.32	Network & Security Technologies Inc	Disagree	Suggest requiring changes be tested for all High and Medium Impact Cyber Systems. Requirements to use a test environment that models production environment and to document differences could be applied only to High Impact systems in Control Centers.
41.33	Midwest ISO	Disagree	The requirement to document changes to the inventories in R23 is 30 days. The requirement to update inventories CIP-010 R2 is 45 days per CIP-010 R2. These should be consistent and we recommend it should be 60 days per our response in Q5.
41.34	APPA Task Force	Disagree	We propose the following changes to the Impact Levels of R23 if our changes proposed in Question 40 are accepted:R23 Table 23.1: Low Impact: Required for Control Centers OnlyMedium Impact: N/AHigh Impact: N/AR23 Table 23.2: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: Required for Control Centers OnlyR23 Table 23.3: Low Impact: Required for Control Centers OnlyMedium Impact: N/AHigh Impact: N/AR23 Table 23.4: Low Impact: N/AMedium Impact: Required for Control Centers OnlyHigh Impact: Required for Control Centers

#	Organization	Yes or No	Question 41 Comment
			OnlyR23 Table 23.5: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.6: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.7: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyR23 Table 23.8: Low Impact: RequiredMedium Impact: RequiredHigh Impact: Required
41.35	GTC & GSOC	Disagree	We recommend that R23.7 be applicable for control centers only. This requirement is more appropriate for control centers and not for transmission and generations operations. While this requirement may be feasible for certain types of protective relays, this technology generally does not exist for a wide range of devices including certain RTUs and meters. In fact, some RTU's must be taken offline in order to retrieve their configuration. Thus, compliance with this requirement would have a negative reliability benefit.
41.36	Progress Energy (non-Nuclear)	Disagree	We see 23.5 as documented lab and field testing for any change to an existing relay/gateway/etc. configuration. Is this what was intended?Baseline configuration is not clear - does this start with the implementation date of the standard or the original production of the facility/element.Virtual BES is not clear. Please specify intention.

42. The definition of sensitive information was derived from the previous version of the CIP standards to minimize disruption to entity information protection programs that are already in place. Do you agree with the proposed definition? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

The definition of "sensitive information" that was originally posted as an informal definition adjacent to Requirement R24 in the draft CIP-011-1 was:

For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.

The primary issue identified with sensitive information was the term itself. Many commenters indicated that this term is already being used by organizations for other purposes, and its inclusion in the NERC CIP standards will cause much confusion. There were several suggestions of alternative terms to use including "CIP-sensitive information" and "protected information." In response to these comments, the drafting team has changed the term to "BES Cyber System Information." The commenters also included numerous suggestions for the improvement of the definition. One commenter indicated that this was not really a definition at all, but rather a list of examples. The drafting team did recognize this as a list of examples, and as such removed it from the requirement language and included the suggestions in the definition of the term BES Cyber System Information.

Several commenters indicated that "floor plans of computing centers" should be removed from the definition. The drafting team agrees that floor plans are problematic as they often are required to be submitted as part of work permits or other items. As such, the drafting team has clarified that only those floor plans that include impact designations of BES Cyber Systems should be identified as BES Cyber System Information, since it is the aggregate data that rises to the level of required protections and not just floor plans alone. This modification was also made to other elements of the definition such as equipment layouts.

A few commenters suggested that the scope of the definition was not broad enough and should be modified by saying "includes but not limited to" or changed entirely to include all data that affects the confidentiality, integrity, and availability of the BES. The drafting team appreciates this suggestion, but sees difficulty in the ability to measure such a broadly scoped definition. Additionally, the drafting team wanted to base the definition on the elements previously defined in CIP-003-3 R4.1 to leverage the investment that Responsible Entities have already made in their existing NERC CIP Information Protection Programs.

The proposed definition of "**BES Cyber System Information**" is:

"Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans."

#	Organization	Yes or No	Question 42 Comment
42.1	Florida Municipal Power Agency	Agree	24.4 - How can a RE "revoke access" from data which may have been copied by personnel?
42.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
42.3	CWLP Electric Transmission, Distribution and Operations Department	Agree	Does network topology or similar diagrams include in-house wiring or plant wiring that may include fiber and Ethernet facilities?
42.4	Exelon Corporation	Agree	Exelon seeks clarification on the following question. Is it the intention of the Standard Drafting Team to include blueprints (schematics and one lines diagrams) for relay and SCADA components in the definition of sensitive information? And, to the extent that such information described large generation facilities or combinations of facilities greater than 2000 MW, then would the electronic record system be considered a High BES Cyber System?
42.5	USACE - Omaha Anchor	Agree	Question - it's difficult to electronically distribute controlled information - however the incident response plan and the recovery plan are supposed to be easily available to all folks. Seems a bit of an oxymoron.

#	Organization	Yes or No	Question 42 Comment
42.6	Northeast Utilities	Agree	The prior version had a concern with user lists, logon-ids, etc. Was applicability to that type of information intentional removed? Also, please clarify whether a recipient of CIP sensitive information must be CIP cleared (PRA & trained).
42.7	Consultant	Disagree	"...network topology or similar diagrams..." should be modified to "network topology that includes BES Cyber Systems" Corporate network topology should not be included in the standards, but this wording would include such diagrams."...floor plans of computing centers that contain BES Cyber Systems..." should be removed, or clarified to specify "floor plans that indicate locations of BES Cbyer Systems". Building floor plans exist in many places that are beyond the control of the Responsible Entities, e.g. architects, landlords, building maintenance companies. A better option might be rewording to qualify the entire list of items as applying to BES Cyber Systems. "... includes (1) security operational procedures, (2) network topology or similar diagrams, (3) floor plans of computing centers, (4) equipment layouts, (5) disaster recovery plans, (6)incident response plans, and (7) security configuration information that contain BES Cyber System information.The definition should be written as a definition, i.e. Sensitive Information - (1) security operational procedures, (2) network topology or similar diagrams, (3) floor plans of computing centers, (4) equipment layouts, (5) disaster recovery plans, (6)incident response plans, and (7) security configuration information that contain BES Cyber System information.The definition is NOT 'For the purposes of this standard', it is expected to be included in the next Glossary update after approval of the standard, and the defined term is hidden somewhere in the statement.
42.8	Luminant	Disagree	"floor plans of computing centers that contain BES Cyber Systems" should be changed to "floor plans that specifically identify BES Cyber Systems or their locations". " BES Cyber System disaster recovery plans" should be “BES Cyber System recovery plans"
42.9	Tenaska	Disagree	24.1 should say: Identify sensitive information.24.2 should say: implement procedures protect sensitive information25.1 should say: render sensitive information unusable

#	Organization	Yes or No	Question 42 Comment
			when disposing of documents and equipment that may contain that information.
42.10	Alliant Energy	Disagree	Alliant Energy agrees with EEI on all points and timeframe consistency. Table 24 is another occurrence where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement.
42.11	Dairyland Power Cooperative	Disagree	BES systems actually contain information/data about the BES that is sensitive as well, but are ignored. Definitions for SCADA, electrical network topology, schematics, and other information can also be BES information related to critical infrastructure that requires protection.
42.12	E.ON U.S.	Disagree	CIP-011, R24 The definition of sensitive information should provide examples of what constitutes a “security operational procedure.”
42.13	CenterPoint Energy	Disagree	Disagree - CenterPoint Energy believes the Responsible Entity should identify and classify data as sensitive information and therefore the definition is too restrictive. CenterPoint Energy recommends it be revised as follows: For the purpose of this standard, sensitive information includes but is not limited to, security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and

#	Organization	Yes or No	Question 42 Comment
			security configuration information.
42.14	Dominion Resources Services, Inc.	Disagree	Dominion recommends changing “contain” to “identify” and adding the phrase “that specifically identify Medium or High Impact components” after the phrase “equipment layout of BES Cyber Systems.” This modification is reflected in the revised definition below: For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that identify BES Cyber Systems, equipment layouts of BES Cyber Systems that specifically identify Medium or High Impact components, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.
42.15	Bonneville Power Administration	Disagree	FERC, NERC and the Regional Entities do not have the information necessary to determine what information is sensitive or not as it regards any Responsible Entity. This is conditional and depends on more that just the types of information involved. The determination of what is sensitive information, and what is not can only be done by the Responsible Entity and under the laws and regulations they must comply with. Floor Plans, network diagrams, equipment layouts and other information may or may not be sensitive depending upon what additional information is provided with it. In addition, legal contracts, Federal, state and municipal laws, regulations, and fiduciary requirements may also govern what information may be protected and what must be released.Recommended Change - For the purpose of this standard, sensitive information may include security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information as determined by the Responsible Entity.
42.16	NextEra Energy Corporate Compliance	Disagree	In R24, is it a requirement to map every user's access privileges to sensitive information?In R24, for every new document that contain security operational procedures, network topology or similar diagrams, floor plans of computing centers

#	Organization	Yes or No	Question 42 Comment
			that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information, do we need to record the explicit authorization of every personnel that has access privileges for each type of documents?In 24.2, does this mean that the handling procedures for hard copies of sensitive information include a documentation for chain-of-custody for High Impact BES Cyber Systems?
42.17	Regulatory Compliance	Disagree	Incident Response plans and Diaster and Recovery plans should not be included as sensitive information - these plans should be psuedo public as long as they have written without security configuration information in them.
42.18	Progress Energy (non-Nuclear)	Disagree	It is not clear if this includes relay device information such as electrical diagrams/schematics.Incident response plans typically do not contain any system specific information. The plans provide the actions that must be taken and must be freely available to many. Will that approach meet the intention of the new standard?
42.19	MidAmerican Energy Company	Disagree	Many entities including MEC use "Sensitive" information as one of the classifications for information that needs to be protected. Calling all information to be protected sensitive will cause confusion. Change the term "sensitive information" to "protected information" in CIP-011.
42.20	Con Edison of New York	Disagree	o R24.3 does the word explicitly mean we cannot say all EMS staff has access to information? Does it need to be by name?
42.21	Network & Security Technologies Inc	Disagree	R24 and/or its sub-requirements should be modified to make it clear they apply sensitive information regardless of media type (including paper copies).24.4 - Revocation of access can be hard to do, and even harder to verify, in cases where an individual has taken either electronic or paper copies of sensitive documents off the Responsible Entity premises (sometime for legitimate reasons). Suggest revising this requirement in a manner that acknowledges this reality - something like “best effort” to retrieve sensitive information the individual may have in his or her possession,

#	Organization	Yes or No	Question 42 Comment
			accompanied by warnings that subsequent unauthorized disclosure of any such information may result in prosecution.
42.22	Hydro One	Disagree	Recommend that the definition change “includes” to “includes but not limited to”.
42.23	ISO New England Inc	Disagree	Recommend that the definition change “includes” to “includes but not limited to”
42.24	Northeast Power Coordinating Council	Disagree	Recommend that the definition change “includes” to “includes but not limited to”.
42.25	US Army Corps of Engineers, Omaha Distirc	Disagree	Remove "floor plans of computing centers"
42.26	Allegheny Energy Supply	Disagree	Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram “similar” (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security

#	Organization	Yes or No	Question 42 Comment
			configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part of this standard.
42.27	LCEC	Disagree	Sensitive is a classification that is specific to the CIP standards per this definition but is used in organizations as one of the levels of information classification. To differentiate, the term BES Sensitive might be considered.
42.28	Public Service Enterprise Group companies	Disagree	Sensitive should be changed to “protected Information”, the definition is fine.
42.29	Progress Energy - Nuclear Generation	Disagree	Sensitivity levels for information are established for nuclear generation facilities by CFR. This definition should be adjusted to acknowledge information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
42.30	Southwest Power Pool Regional Entity	Disagree	Should include more than “security” operational procedures. IT-specific operating procedures (“run books”) are very sensitive and could be used to exploit a system. Operations procedures may also be sensitive to some extent if they describe the use of the BES Cyber System.
42.31	San Diego Gas and Electric Co.	Disagree	The "definition" is only a list of examples, not a real definition. SDG&E suggests the following definition: "Sensitive information is defined as any information owned by

#	Organization	Yes or No	Question 42 Comment
			the Responsible Entity, or for which the Responsible Entity is the custodian of, that, if inappropriately disclosed, modified, or rendered unavailable, could adversely impact human safety or the reliability of the BES. Examples include...(their list)"
42.32	APPA Task Force	Disagree	The APPA Task Force would like to comment on the definition of sensitive information: As pointed out in Question 44, the following disclaimer needs to be added to that definition: "To the extent that state/local laws allow"
42.33	Entergy	Disagree	The definition of sensitive information is nearly identical to the one currently being used in version 3. R24.1 and R24.2 explicity allow the Entity to classify and protect "sensitive" information under its own auspice. As long as the classification guidelines are left for the Entity to decide, this definition should prove sufficient.The requirement indicates that the drafting team believes protection of sensitive information associated with allegedly "low impact" BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.Please define "Explicitly Authorize"? Does this mean that every individual with access to a particular piece of information needs some type of documented approval? Can this be done at a group level based on job function? Is approval documentation all that's required, or is a maintained list required as well?
42.34	Manitoba Hydro	Disagree	The definition should also reference control rooms.
42.35	Southern California Edison Company	Disagree	The definition should clearly distinguish BES operational information and cyber security related information. A smaller subset of the former and larger subset of the latter form potential candidates for "protected information".
42.36	Oncor Electric Delivery LLC	Disagree	The definition should not prescribe items as being "sensitive". The identification and classification process of Requirement 24.1 should do that. "For the purpose of this standard, sensitive information includes procedures, diagrams and any other document which provides proprietary information about BES Cyber Systems or BES

#	Organization	Yes or No	Question 42 Comment
			Cyber System Components."
42.37	Allegheny Power	Disagree	There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part

#	Organization	Yes or No	Question 42 Comment
			of this standard.
42.38	EEI	Disagree	There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part

#	Organization	Yes or No	Question 42 Comment
			of this standard.
42.39	ReymannGroup, Inc.	Disagree	This definition should be expanded to include the identification and classification of ALL data that affects the confidentiality, integrity, and availability (CIA) of the BES system commensurate with its sensitivity and consequence.
42.40	US Bureau of Reclamation	Disagree	This effort needs to be aligned with the Executive level CUI requirements.
42.41	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
42.42	We Energies	Disagree	We Energies agrees with EEI: There is no reasoned basis to simply bring forward a historic definition then add significant additional requirements based on a legacy definition.We Energies agrees with EEI: Requirement 24.3 is in conflict with 24.1 and 24.2 as it brings specific obligations that may or may not be appropriate.We Energies agrees with EEI: The existing definition of sensitive information:For the purpose of this standard, sensitive information includes security operational procedures, network topology or similar diagrams, floor plans of computing centers that contain BES Cyber Systems, equipment layouts of BES Cyber Systems, BES Cyber System disaster recovery plans, BES Cyber System incident response plans, and security configuration information.is overbroad and inappropriate. We Energies agrees with EEI: A corporate procedure or signage indicating that visitors to a facility must register their presence could be considered a security operational procedure, and be considered sensitive information. A diagram "similar" (but not identical) to a network topology diagram, even if written on the back of a napkin, could be considered sensitive information. Floor plans are routinely required to be filed (generally publically) by municipal building and zoning authorities before construction permits are issued. Elements of BES Cyber System incident response plans such as local or regional law enforcement personnel contact information should be made widely available to responsible entity personnel. Elements of incident response plans that call for the protection of human life and safety as a primary directive should be made widely

#	Organization	Yes or No	Question 42 Comment
			available to responsible entity personnel. Acceptable Use Banners could be considered part of security configuration information.We Energies agrees with EEI: The definition of sensitive information and associated requirements needs extensive revision. Before beginning, the revision, some effort should be invested to define the security objective. We Energies agrees with EEI: For example the objective may be to prevent an unauthorized party from receiving information that could directly lead to the compromise of BES Cyber Systems. To achieve this objective, it would be desirable to protect BES Cyber System passwords. It may also be desirable to protect documents that provide a complete listing of BES Cyber System dial-in numbers or TCP/IP addresses. Operational plans to protect certain information must reasoned and be balanced with other requirements e.g. the training requirements that are part of this standard.
42.43	American Transmission Company	Disagree	We propose deleting “floor plans of computer centers” from the definition of sensitive information. Floor plans do not typically include information specific to devices, IP addresses, etc which could be used to compromise a BES Cyber System. Moreover, a computer center is an undefined term which could mean anywhere there was more than one computer.
42.44	LADWP	Disagree	Word sensitive needs to be changed as it can coincide with actual classification used by entities.
42.45	FirstEnergy Corporation	Disagree	Would like to see the definition even more narrow, to focus on information that truly can compromise the BES (e.g. Vulnerability assessments’, mitigation strategies, passwords, and DR plans).

43. Do you agree with the proposed definition of Media? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

The definition of "media" that was originally posted as an informal definition adjacent to Requirement R25 in draft CIP-011-1 was:

Media for the purpose of this standard means any mass storage devices within a BES Cyber System Component including, but not limited to, magnetic tapes, optical disks, and magnetic disks onto which information is recorded and stored.

The proposed definition of "media" received significant agreement from those entities that chose to respond to this question. The majority of comments on the definition of media indicated that the definition should be expanded to include additional storage types as well as more traditional media types such as paper. The drafting team intends for Responsible Entities to protect media, such as paper, through the required handling procedures included in the Information Protection requirement.

One commenter indicated that USB drives, CDs, and floppy disks should be included in the definition of media. It was the intent of the drafting team that these device types would be considered devices used to perform maintenance and thus treated in accordance with the maintenance requirements. As the maintenance requirements evolved with the inclusion of additional remote access requirements, the drafting team considered expanding the scope of the media definition.

Another commenter made an interesting case regarding the media being "within" a BES Cyber System and suggested that once the media was removed that it no longer met the definition. The drafting team considered this comment and has modified the standard to require sanitization of BES Cyber System Information contained on media. The remaining comments focused primarily on the requirements themselves and not the definition. Specifically, commenters were concerned about the level of sanitization that would be required on the media. Several commenters noted that the level of sanitization should be commensurate with the potential threat to BES reliability, while others suggested that there be a defined minimum acceptable sanitization process, such as an NSA standard. The drafting team understands the need for a minimum acceptable sanitization process. However, the NERC Standards Development Process does not allow the drafting team to simply reference another standard. As such, we have modified the language in the revised standard to require that media be destroyed or other actions taken to prevent unauthorized retrieval.

Given the potential confusion with establishing a NERC Glossary definition for media, the drafting team has elected to define the term within the language of the standard itself.

#	Organization	Yes or No	Question 43 Comment
43.1	Florida Municipal Power Agency		How would one define the process used to render the media unrecoverable? What does unrecoverable mean? Unrecoverable by NSA standards or unrecoverable by means of something like phase transition?
43.2	Black Hills Corporation	Agree	Believe that solid-state mass-storage (flash drives, thumb drives, jump drives, etc,) should be included as examples in the definition.
43.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
43.4	Northeast Utilities	Agree	Suggest that a minimum acceptable sanitization process (i.e., NIST standard) is specified.
43.5	APPA Task Force	Agree	The APPA Task Force agrees with the definition.
43.6	Dairyland Power Cooperative	Agree	With the proliferation of flash memory solutions, the only way to sanitize some media is physical destruction. Many devices use flash memory in a way that is not removable. Is destruction of this equipment intended?
43.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
43.8	FirstEnergy Corporation	Disagree	Believe the definition should not include example because of the quickly changing storage technologies.
43.9	Xcel Energy	Disagree	Further clarification, similar to the definition of Maintenance in R26, is needed to make it clear that media such as hard drives on laptops used for maintenance do not need to be sanitized after temporary connection to BES Cyber Systems.

#	Organization	Yes or No	Question 43 Comment
43.10	LADWP	Disagree	Is portable storage included here?
43.11	Emerson Process Management	Disagree	It should include USB memory stick which is becoming very popular.
43.12	LCEC	Disagree	Media can be removed from the BES Cyber System and it should still be considered media per this requirement. Remove the word "within" and replace with "used by" or "written to by" a BES Cyber System.
43.13	Public Service Enterprise Group companies	Disagree	Media should also include persistent configuration data that is stored in solid state devices (e.g. flash memory, EEPROM (electrically-erasable programmable read-only memory), etc.)
43.14	Southwest Power Pool Regional Entity	Disagree	Portable media, including CD/DVD and USB devices should be included. Basically, anything that sensitive information can be written to.
43.15	Reliability & Compliance Group	Disagree	Recommend removing the word “mass” and instead use the term storage devices.
43.16	USACE - Omaha Anchor	Disagree	Sanitization should only apply to media internal to the devices.
43.17	San Diego Gas and Electric Co.	Disagree	SDG&E notes that the proposed definition does not appear to include "old school" media like paper that is often used to store sensitive information.
43.18	ERCOT ISO	Disagree	Should also specifically address CDs and USB storage devices in the definition.
43.19	Progress Energy (non-Nuclear)	Disagree	Should the definition also clearly state device hard drives?
43.20	Manitoba Hydro	Disagree	The current definition would also require the sanitization of other mass storage devices, such as flash memory, which could render the cyber component unfit for

#	Organization	Yes or No	Question 43 Comment
			reuse outside of the BES Cyber System. The strict sanitization requirement does not permit the return of a failed BES Cyber System or BES Cyber System Component to the vendor for failure analysis. The information protection requirements must provide more flexibility, which may also be achieved through processes and procedures.
43.21	ReliabilityFirst Staff	Disagree	The definition does not need to specify “mass storage devices” and, in fact, should include devices such as flash drives. Media should also be defined to include media types other than electronic such as paper.
43.22	Consultant	Disagree	The definition is technology limited by magnetic and optical technologies. While pervasive, there are and will be other technologies to retain information.Suggest: Media - computer components and recording media that retain digital data used for computing for some interval of time.Might also consider making the definition "Electronic Media" to eliminate books, notebooks, paper, etc. which are also 'information storage media'.
43.23	Entergy	Disagree	The definition of "media" includes the open-ended term "including, but not limited to", which could practically bring anything into scope. A more concise definition with specific examples would remove ambiguity and leave less room for interpretation. The examples of Media in the box should also include flash memory as well.An example of the type of sanitization required should be provided.
43.24	Alberta Electric System Operator	Disagree	The definition states “including, but not limited to,”. The AESO suggests modifiying the definition to explicitly include non-volatile storage to ensure coverage of memory cards and flash drives.
43.25	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI’s comments.
43.26	We Energies	Disagree	We Energies agrees with EEI: When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of

#	Organization	Yes or No	Question 43 Comment
			voltage or frequency does not pose a risk to the BES.
43.27	Allegheny Energy Supply	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of ambient air temperatures does not pose a risk to the BES.
43.28	Allegheny Power	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
43.29	EEI	Disagree	When writing the definition, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.

44. Requirements R24 and R25 of draft CIP-011-1 concern procedures for information protection and media sanitization. Do you agree with the list of criteria that are included in each Requirements Table for R24 and R25? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

Concerns regarding the requirement for information protection centered around the revocation timeline and scope as well as differentiating access to information vs. access to systems. The drafting team is attempting to address the FERC directive that requires the revocation of access to BES Cyber System Information. The drafting team is proposing to address revocation of access to BES Cyber Systems and to BES Cyber System Information all in one place to ensure more consistency in the requirements and their implementation.

There were a number of commenters who raised concerns with the requirement for media sanitization regarding media failure conditions or disposal. The word "sanitization" appeared to cause confusion for a number of commenters and as such has been removed from the revised standard. Additionally, a couple of commenters raised concerns about the burden of proof, compliance requirements, legal issues, and ownership responsibilities.

As with other areas of this standard, there were a significant number of the comments asking for clarity of phraseology and terminology, including words such as consequence, annually, explicitly, acceptable, commensurate, etc. The drafting team eliminated the words, "explicitly, acceptable, commensurate, and annual" from the revised CIP-011-1 standard.

#	Organization	Yes or No	Question 44 Comment
44.1	ISO New England Inc		Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for causeWhat about revoking access for other than cause?Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing "reuse outside of BES Cyber Systems" to "reuse outside of the Entity's High Impact or Medium Impact BES Cyber Systems"
44.2	Northeast Utilities	Agree	Agree that this requirement covers the key cyber assets but how does this apply to

#	Organization	Yes or No	Question 44 Comment
			protective systems such as the physical access system, firewalls and logging devices?
44.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
44.4	Black Hills Corporation	Agree	Legally Required Release: There may be "legal" situations in which we may be required to share certain information with outside entities, both government and non-government. Examples could include OSHA or MSHA investigations, employee lawsuits (with the associated discovery). There does not appear to be any provision in the regulation to allow this sharing. We could be placed in the position of violating this regulation, or violating some other legal requirement (subpoena, etc)
44.5	Puget Sound Energy	Agree	Puget Sound Energy suggests modifying R24.4 to "Revoke access to media containing sensitive information within 24 hours..." to align with the NERC definition in R25 and to provide clarity around sensitive information in a hardcopy format.
44.6	GTC & GSOC	Agree	We recommend the verbiage and timelines for R24.4 be consistent with tables R5 and R13.
44.7	Independent Electricity System Operator	Disagree	- R24.4 define for cause. Should the wording be involuntarily terminated to include those that are terminated unwillingly due to layoffs, job cuts, fired/performance, etc.- R24.4 how do you remove access where personnel may have physical copies offsite o
44.8	ERCOT ISO	Disagree	24.2: Recommend: "Implement labeling and handling procedures for sensitive information according to its defined classification level." 24.3: It is unclear whether the requirement includes internal and external personnel. 24.4: Should be combined with other access management requirements (physical, cyber)24.5: Should also address "need to know". The requirement did not address the access control means for protecting information or the access to hard copies of information.
44.9	Duke Energy	Disagree	24.3 - We don't feel it is realistic to explicitly authorize access to paper copies of

#	Organization	Yes or No	Question 44 Comment
			information. Add 'repositories' at the end of the sentence.Include "repository" in 24.4 and 24.5 as well. Requirement 24.3 is particularly burdensome in a nuclear environment where there is already heavy physical security. There are thousands of drawings, for example, available for the plant. There are hundreds of personnel that have a business need to know certain things about the plant that are contained in these drawings. During outages that number often goes above 1000 personnel. Segregating all drawings/manuals/equipment layouts/floor plans/procedures and EXPLICITLY authorizing personnel for access is difficult at best. Certainly, protecting cyber specific information such as firewall rules, group policies, passwords, and other specific cyber information makes sense and is done already.
44.10	Regulatory Compliance	Disagree	24.4 - Strike altogether. Revocation should go back and be included in the scope of System revocation.25.1 - Propose : Sanitize only media containing sensitive information prior to disposal for reuse outside of BES Cyber Systems, using a method to render the data unrecoverable.
44.11	Southwest Power Pool Regional Entity	Disagree	24.4: Is this requirement prescribing Information Rights Management? There are many types of access, including access to information no longer under the direct control of the entity. 24.5 is poorly worded. Would be better to require that access is authorized, not that it reflects authorization. 25.1 should require either sanitization or physical destruction.
44.12	American Electric Power	Disagree	25.1: Regarding "Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a method to render the data unrecoverable", what evidence would be required from an audit perspective? If a USB harddrive is used to copy patches onto a system, would that USB harddrive need to be destroyed with documented evidence if it failed 2 weeks down the road?Suggested rewording:Media for the purpose of this standard means any mass storage devices within a BES Cyber System Component including, but not limited to, magnetic tapes, optical disks, and magnetic disks onto which sensitive information is recorded and stored.Rational: Adding sensitive to the "Media" definition will clarify that this is intended to be used

#	Organization	Yes or No	Question 44 Comment
			to protect the inadvertent distribution of protected information, not all media devices that are plugged into a BES Cyber System will need to be sanitized.
44.13	BCTC	Disagree	Â R24.4. We need clarification on revocation of access. We are assuming it is from the point the person departs their job - i.e. access to the BES Cyber System is revoked. Such personnel could have hard copies of information but how would you prove that such documentation was shredded? What about information they have retained within their brain? ï?Š We need some clarity on what the parameters are herePlease provide a concise definition for 'sanitize'. We discussed scenarios such as patching the BES Cyber System via a CD - would compliance require that we 'sanitize' the CD? If yes, seems like overkill from our discussions on the subject. Please provide more concise language to define the scope.over real time to either. Yet, in reading the requirements we could potentially be found non-compliant based on the wording of the version 4 standards - this should not be! FYI, I raised this point at the recent 2 day workshop in Texas and the drafting team was in agreement that our current configuration is an example of excellence ... yet is a potentially non-compliant based on current wording ... this needs to be revisited.
44.14	Progress Energy - Nuclear Generation	Disagree	Agree with R24.1, R24.2 and R25.1. Disagree with R24.3, R24.4 and R24.5 which are governed for nuclear generating facilities by CFR. R24-24 should acknowledge information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
44.15	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
44.16	E.ON U.S.	Disagree	CIP-011-1, R24.4 is unnecessary and difficult to impossible to document. At this point, all authorized unescorted physical and electronic access would have been removed per other requirements. E ON U.S. proposes that this requirement be deleted.

#	Organization	Yes or No	Question 44 Comment
44.17	USACE - Omaha Anchor	Disagree	Definition would include external hard drives and other external media. It seems ridiculous if you are installing patches to sanitize the media before going to the next cyber system. You are treating the cyber system as a classified system. This is serious overkill. External media for the most part should be exempt from this requirement unless sensitive information is placed on the media in which case it should follow the rules of R24.
44.18	Dominion Resources Services, Inc.	Disagree	Dominion recommends revising Requirement R24.1 to read:"Identify and designate controls for protection of sensitive information commensurate with its importance to the security and reliable operation of the associated BES Cyber System."24.3. With the heavy industry reliance on vendors and contractors and the requirements throughout other NERC standards to share data with other entities, it is impractical to "Explicitly authorize personnel for access to sensitive information." For example, when information is sent outside Dominion, it is impossible to know every person who sees it. Moreover it is unlikely that whoever does see it would want to sign an agreement with every entity that can submit information. The controls specified above in the requested revision to 24.1 should cover the requirements for access to the information. Dominion requests that this requirement be removed.24.4. It is possible to revoke electronic access to company-controlled devices containing sensitive information and to revoke physical access to company-controlled areas containing sensitive information within 24 hours. It is not reasonable to identify and retrieve information within 24 hours that may have been taken by an authorized user prior to being terminated for cause and it may not be possible to ever retrieve this information if it has been hidden by the individual. Please restate this requirement to indicate that it covers physical and electronic access as follows:"24.4 Revoke electronic access to company-controlled devices containing sensitive information and physical access to company-controlled areas containing sensitive information within 24 hours."24.5. As stated in Dominion's comment to 24.3, it is impractical to authorize individuals. As applied to this requirement it is also impractical to track individuals. In the example given in the above response to 24.3, any non-company

#	Organization	Yes or No	Question 44 Comment
			personnel that might see sensitive data would need to be authorized by every Registered Entity and their companies would have to keep every RE appraised of every personnel change and provide annual lists of all personnel. Dominion requests that this requirement be removed.Note: At Dallas, the SDT requested input as to requiring training and a PRA for access to sensitive information. Dominion requests that training and a PRA NOT be required. Training and a PRA are not required by versions 1, 2, and 3 of the CIP standards and could be impossible to implement across vendors within the electric industry. In the example given in the above response to 24.3, every vendor or business partner would have to take the training from every Registered Entity or have their training approved by every entity (including annually providing the training program to each RE for approval) and ES-ISAC would have to keep every RE appraised of every personnel change and provide annual lists of all personnel. And then, PRAs would have to be addressed. Registered Entities should be required to have internal requirements for access to sensitive information.
44.19	ReymannGroup, Inc.	Disagree	Expand the list of procedures to include 3rd party data recovery services in accordance with an approved vendor management policy for all impact levels.
44.20	RRI Energy	Disagree	Explicitly define “access” as related to sensitive information. Data can be locally cached on web browsers, remote or personal pc’s, etc. These cannot easily be removed let alone 24 hrs removal.
44.21	Constellation Power Source Generation	Disagree	In R24.1, what classifications for sensitive information should be used? The SDT should develop classifications specifically for CIP. As written, this is not an auditable requirement.
44.22	ReliabilityFirst Staff	Disagree	In row 24.1, what is meant by “consequence”? In Table R24, row 24.5, we suggest the verification of access privileges be performed at least quarterly. To Table R24, add a new row 24.6 stating, “Revoke access to sensitive information within 72 hours for personnel terminated not for cause.” And assign this requirement an impact level of “Required” for both Medium and High Impact BES Cyber Systems. Table R25, row

#	Organization	Yes or No	Question 44 Comment
			25.1; we believe there should be a definition of “sanitize” to eliminate confusion regarding what actions must be taken to comply with this requirement.
44.23	MidAmerican Energy Company	Disagree	It was mentioned in the May workshop that the SDT would consider the necessity for Personnel risk assessments and training required prior to granting access to protected information.Personnel risk assessments and training should not be required prior to granting access to protected information. As an example, entities would have a nearly impossible task of completing personel risk assessments for international employees at global help desks that are allowed view only access to a BES Cyber System.
44.24	WECC	Disagree	Item 24.2 should be made clear that individual hard drives, servers, laptops, etc do not need to be labeled. Perhaps “labeling of media” was meant. Item 24.3 will have great impact on the ability to have technical support from large global vendors such as Cisco. Consider exception to this requirement for maintenance or add something to Maintenance requirement R26 to deal with it.Clarify how sensitivity and consequence are determined.Clarify the requirements for authorization for access to sensitive information (i.e. need to know).
44.25	LCEC	Disagree	Need to clarify the acceptable methods.
44.26	NextEra Energy Corporate Compliance	Disagree	NextEra believes that R24 did not take into consideration access privileges with sensitive information. It does not provide clear guidance and left room for interpretation. The following are the recommended updates:R24.5 Verify at least every 12 months that the access privileges to sensitive information reflect the appropriate need with the personnel roles and responsibilities. Access privileges to sensitive should correspond with the needs and appropriate personnel roles and responsibilities.Regarding CIP-011-1/R25, R25 did not provide a standard to sanitize media. The current language did not provide clear guidance and left room for interpretation. The following is the recommended updates:25.1 - Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using clearing

#	Organization	Yes or No	Question 44 Comment
			utility supporting the Department of Defense clearing and sanitation standard. R24.4 - Requirement covered by revocation of physical and cyber access.Revoking physical and cyber access would revoke access to protected information. Therefore, NextEra suggests removing 24.4
44.27	National Grid	Disagree	o Provide timelines for access revocation for reasons other than "terminated for cause" o Do laptops and devices that maintain the BES Cyber Systems need to be sanitized?
44.28	PacifiCorp	Disagree	PacifiCorp asks that the reference to "at least every 12 months" is modified to read "annuallyonce every calendar year." Allowing responsible entities the flexibility to require trying once every calendar year rather than at least every 12 months would relieve entities of the significant administrative burden of tracking specific training deadlines for each individual employee. At the same time, this change will still ensure that employees are trained at regular enough intervals to achieve the reliability goal of the training requirement.
44.29	Ameren	Disagree	R24.3 - Listing people who have access to information serves no purpose in protecting BES systems from Cyber attack. The list of people with this information is not the same as the list of people that have access to the systems. This requirement should be removed.R24.4 - This requirement is impossible to prove for printed documentation. Suggest removal.
44.30	Liberty Electric Power, LLC	Disagree	R25 appears to require the hard drives of laptops used in relay calibrations to be wiped before leaving site. This is a serious issue for smaller entities, due to almost all of the relay work being done by outside contractors. These contractors often need the data taken to write reports which are required by other NERC standards. This requirement needs to be removed.
44.31	Allegheny Energy Supply	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to

#	Organization	Yes or No	Question 44 Comment
			perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of ambient air temperature does not pose a risk to the BES.
44.32	Allegheny Power	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
44.33	EEI	Disagree	R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the responsible entity is unable to perform sanitization on the media.Requirement 25.1 uses the word “Unrecoverable”. This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.

#	Organization	Yes or No	Question 44 Comment
44.34	Hydro One	Disagree	Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for cause.Revoking access for other than cause should be addressed.Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing “reuse outside of BES Cyber Systems” to “reuse outside of the Entity’s High Impact or Medium Impact BES Cyber Systems”.
44.35	Northeast Power Coordinating Council	Disagree	Recommend changing 24.4 to Revoke physical/logical access to sensitive information for personnel terminated for cause.Revoking access for other than cause should be addressed.Recommend changing R25.1 to avoid the gap of High Impact to Low Impact to reuse outside of BES Cyber Systems. Suggest changing “reuse outside of BES Cyber Systems” to “reuse outside of the Entity’s High Impact or Medium Impact BES Cyber Systems”.
44.36	Idaho Power Company	Disagree	Revocation of access to sensitive information is virtually impossible if the person terminated has the information in their possession either hard copy or portable media. Access to additional information can be revoke. Consider rewording this requirement to accommodate this reality.
44.37	Southern California Edison Company	Disagree	SCE feels the standard, as written, may be operationally difficult to implement. As such SCE recommends allowing for the revocation of electronic access to sensitive information within 24 hours, or make a written demand (which may be followed up by legal process) for such information within a 24 hour timeframe. This distinction is crucial as not all sensitive information may reside within the physical confines of the registered entity. Business concerns may require registered entities to allow sensitive information (if adequately protected by contractual or employment terms) to leave the confines of the company. For example, employees may have CIP-protected information in company-issued laptops. In some scenarios, it may be impossible to recover those laptops if they were left offsite when the employee was terminated. However, it would be possible to issue a written demand, supported by law, for such

#	Organization	Yes or No	Question 44 Comment
			documents. The drafting team is requested to rephrase R24.4 with a view on implementability, enforceability and auditability.
44.38	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that R24.3 should read "Explicitly authorize role-based access to sensitive information."In R24.4, SDG&E asks how would we do this for hard-copy information?In R24.5, SDG&E suggests changing the wording to read "Verify at least every 12 months that the role-based access privileges to sensitive information reflect authorization."
44.39	Progress Energy (non-Nuclear)	Disagree	Should there be an item in table R25 to identify the media to be sanitized that may be overlooked, i.e. printers/plotters/scanners, relay test sets, etc.
44.40	Consultant	Disagree	Table R24 - Item 24.3 This is an access control requirement, and should be moved to access control requirement table. Access control should cover cyber access, physical access, and information access together, as the process for attaining each type of access is related.Item 24.4 is an access revocation requirement, and should be moved to the access revocation requirement table. Access revocation should cover cyber access, physical access, and information access together, as the process for revoking each type of access is related. The comments related to timeframes in those sections are applicable to information access revocation as well.Item 24.5 is an account management requirement, and should be moved to the account management requirement table. Account Management and reviews should cover cyber access, physical access, and information access together, as the process for reviewing and confirming each type of access is related. The comments related to timeframes in those sections are applicable to information access access review as well.Table R26 - Item 26.1 Replace the word "all" with "BES Cyber System" as a better statement.Item 26.1 If 'media' is a defined term it should be capitalized. (See comments on definition of Media.)
44.41	APPA Task Force	Disagree	The APPA Task Force cautions the drafting team on the information protection requirements in R24. Nearly every state in the United States has a public records law

#	Organization	Yes or No	Question 44 Comment
			that applies to public power systems as units of state or local government (These laws are often referred to as “Government in the Sunshine” laws.). We recommend that the drafting team consult with NERC legal counsel prior to revising this requirement. We do not want public power systems to have to choose between being in noncompliance with the proposed requirements or violating their state open records laws. Rebecca Michaels of NERC Staff is familiar with this issue. If this must move forward as proposed we recommend that the following be added to the requirement: “To the extent that state/local laws allow.”R24.Objective:To prevent unauthorized access to sensitive information associated with BES Cyber SystemsR24. Requirement:To the extent permissible under federal and state laws, each Responsible Entity shall document and implement one or more processes that incorporate the criteria in CIP-011-1 Table R24 - Information Protection.
44.42	Reliability & Compliance Group	Disagree	The method of sanitizing media should be done in an industry accepted manner to provide for auditability of the standard.
44.43	Bonneville Power Administration	Disagree	The objectives of these requirements (“to prevent unauthorized access to sensitive information associated with BES Cyber Systems” and “to prevent the unauthorized dissemination of BES Cyber System information”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R24, Section 24.1. Recommend replacing "classify" and "classification" with "categorize" and "category" and "categorization", . "Classify" and "classification" have very specific meanings to any Federal agency. Those meanings are restricted to the realm of National Security Information and are different from what is presented here. Such information requires storage in General Services Administration-approved safes, transmission using National Security Agency-approved encryption, and can be only be processed on computer systems if those systems are dedicated to such use, totally isolated from any publicly accessible network, and stored in secure facilities when not

#	Organization	Yes or No	Question 44 Comment
			in use. Furthermore, the Federal Agencies do not have the option of using a different definition. In fact, using Regional Entity standard forms marked "Confidential" is problematic for Federal agencies, as such a marking is reserved for a particular level of classified information. Given the large number of Federal organizations to which this standard applies, it would simplify matters to restrict the use of "classify" and similar terms to the realm of National Security Information.Recommend deletion of Table 24, Section 24.3. Requiring formal authorization is a process more stringent to that required to gain access to National Defensed Information at the Confidential and Secret level: A formal determination of trustworthiness, but no formal further formal authorization required for access once the clearance has been granted. For sensitive information other than National Defense Information, Federal agencies are required only to determine the the recipient needs the information to support the activities of the agency. Such a determination can be made informally, by any person with custody of the information. We realize that there seem to be conceptual difficulties about revoking access without formally authorizing it. But, they are resolved when we note that authorizing access is not the same as granting it. Authorizing access is a declaration that the person is allowed to have access. Granting access is giving them the info. It is not clear to which of these "revoke" is intended to apply. However, R24 is only concerned about revocation following termination for cause. In those cases, electronic and physical access to all Entity assets is generally revoked. That would effectively deny access to the information, as well. Thus, revocation can be accomplished even though a formal access authorization is not used.
44.44	US Bureau of Reclamation	Disagree	The use of the term classification is not appropriate, suggest "categoruize" to avoid conflict with other requirements in the federal sector.
44.45	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments regarding Requirement 25.1.
44.46	We Energies	Disagree	We Energies agrees with EEI: R25 Needs to contemplate how organizations should handle situations where media has failed or is failing to operate properly and the

#	Organization	Yes or No	Question 44 Comment
			responsible entity is unable to perform sanitization on the media.We Energies agrees with EEI: Requirement 25.1 uses the word "Unrecoverable". This creates an unreasonable mandate for responsible entities to be measured against. Suggest alternative along the lines: Sanitize all media prior to disposal or release for reuse outside of BES Cyber Systems, using a methods, tools or techniques to render BES Cyber System information such as passwords unavailable using commercially available means.We Energies agrees with EEI: When writing the requirement, it is appropriate to consider the threat to BES reliability that is to be mitigated. A series of measurements of voltage or frequency does not pose a risk to the BES.
44.47	FirstEnergy Corporation	Disagree	We would like to have clearer definition on what is acceptable sanitation methods.
44.48	Entergy	Disagree	What exactly does "Explicitly Authorize" mean? Does this mean that every individual with access to a particular piece of information needs some type of documented approval? Can this be done at a group level based on job function? If so, it should be stated as such.Is approval documentation all that's required, or is a periodically maintained list required as well?What is the definition of "Revoking Access"? Does the individual need to be removed from every Cyber System he/she had access to?
44.49	Manitoba Hydro	Disagree	What is the meaning of "consequence" in Requirement R24.1? There is currently no requirement for revocation of access to sensitive information for any other reason than "for cause". There are no specifics given with respect to "classify" sensitive information in Requirement R24.1 so it is assumed to be at the Responsible Entity's discretion in terms of criteria, methodology, etc. There are no specifics given with respect to "method" in Requirement R25.1 so it is assumed to be at the Responsible Entity's discretion.

45. Tables R24 and R25 provide direction concerning what impact level of BES Cyber Systems to which Requirements R24 and R25 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Information Protection and Media Sanitization" is now addressed in CIP–011–1 — Cyber Security — Information Protection.

Concerns were raised by commenters regarding the applicability of the information protection and media sanitization requirements. The issues centered around the tables being too broad brushed. There was also concern surrounding the differentiation of information sensitivity vs. impact categorization. The drafting team modified the standard to only include information protection for High and Medium Impact BES Cyber Systems and associated Physical Access Control Systems, associated Electronic Access Control or Monitoring Systems, and associated Protected Cyber Assets.

#	Organization	Yes or No	Question 45 Comment
45.1	WECC		Criteria should apply to all impact levels
45.2	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
45.3	Consultant	Agree	Table R24 - Items 24.3, 24.4, & 24.5 should be moved to their respective subject areas as suggested in the comment on Question 44. (Cyber access, physical access, and information access requirements should be addressed together, as the requirements and processes for each type of access is related.)
45.4	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R24-R25 if it is understood that a blank in the table means N/A.
45.5	PacifiCorp	Disagree	: Lines 24.1 and 24.2 imply that multiple classifications levels for "Sensitive Information" will be required. Need to allow for entities to use one classification for "Sensitive Information".24.4 The requirement to revoke access to sensitive information within 24 hours is impractical. The information may be offsite on paper hardcopy or electronically on media. 24.5 Entities should also be required to correct

#	Organization	Yes or No	Question 45 Comment
			access privileges found to be inaccurate once they have been verified.
45.6	Southwest Power Pool Regional Entity	Disagree	24.1, 24.2, and 25.1 should be applicable to all impact categories.
45.7	US Army Corps of Engineers, Omaha Distirc	Disagree	24.3 does a job description constitute "explicit authorization?" Restrictions on media use as written would preclude using media to transfer information to external systems using media. Should be reworded with the intent that the media be sanitized before disposed of or released outside the organization or allowances made for transfering information. Also could be interpreted to mean an update disk used to update BES Cyber System 1 would have to be wiped and could not be used to update system 2.
45.8	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
45.9	Allegheny Energy Supply	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.10	Allegheny Power	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.11	EEI	Disagree	As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.
45.12	MidAmerican Energy Company	Disagree	Lines 24.1 and 24.2 imply that multiple classifications levels for “Sensitive Information” will be required. Need to allow for entities to use one classification for “Sensitive Information”.24.4 The requirement to revoke access to sensitive information within 24 hours is impractical. The information may be offsite on paper hardcopy or electronically on media. 24.5 Entities should also be required to correct access privileges found to be inaccurate once they have been verified.

#	Organization	Yes or No	Question 45 Comment
45.13	American Municipal Power	Disagree	Please provide a little or no impact category
45.14	US Bureau of Reclamation	Disagree	Requirements should be applied to information sensitivity, not the impact level of the system(s).
45.15	Southern California Edison Company	Disagree	SCE feels that R24 and R25 apply regardless of the BES Control System impact level.
45.16	Progress Energy (non-Nuclear)	Disagree	See comment 14.
45.17	LCEC	Disagree	See previous comments
45.18	BCTC	Disagree	See Question 44 response
45.19	Bonneville Power Administration	Disagree	See the response to question 44.Item 24.5 in Table R24 states as follows: "Verify at least once every 12 months that the access privileges to sensitive information reflect authorization". Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently verifications must occur.
45.20	LADWP	Disagree	Should be restricted to high level only.
45.21	ReliabilityFirst Staff	Disagree	Suggest "Required" for Low Impact in row 25.1.
45.22	Entergy	Disagree	The requirement indicates that the drafting team believes that protection of sensitive information associated with allegedly "low impact" BES Cyber Systems/Components that provide routable protocol attack vector access to control hosts, etc., is unnecessary. Suggest this be rethought.
45.23	Pepco Holdings, Inc. -	Disagree	We agree with EEI's comments.

#	Organization	Yes or No	Question 45 Comment
	Affiliates		
45.24	We Energies	Disagree	We Energies agrees with EEI: As previously documented, the requirements in tables 24 and 25 are overbroad and not appropriate.

46. The BES Cyber System Maintenance requirement is intended to cover the instances where it is necessary to directly connect a device to the BES Cyber System temporarily to perform a support function, provide appropriate controls on the maintenance device to protect the BES Cyber System. Do you agree with the definition of maintenance as provided?

Summary Consideration:

The definition of "maintenance" that was originally posted as an informal definition adjacent to Requirement R26 in draft CIP-011-1 was:

Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of a BES Cyber System. Examples of maintenance activities for BES Cyber Systems include configuration changes, vulnerability assessments, and software patches. Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System.

There were questions and concerns raised by commenters about what is included in the scope of maintenance activities. There were comments that the term "maintenance devices" needs to be defined. In addition, there was a question regarding whether remote access is included as maintenance. There were suggestions that the definition of maintenance should be focused on the temporary connections.

One commenter suggested the following definition: "Maintenance for the purpose of this standard includes any activity requiring the temporary connection of digital equipment (e.g., laptops) capable of altering the configuration of, or introducing malicious code, to the BES Cyber System." The drafting team considered this feedback, and removed the definition of maintenance from the revised standard, and instead focused on temporarily connecting to a BES Cyber System (such as for maintenance) rather than on the activity being performed. (See proposed CIP-007-5 – System Access Control.)

The requirement for Transient Cyber Assets and media in CIP-007-5 R3.4 is intended to ensure that devices used for temporary access to the BES Cyber System (such as for maintenance) do not accidently introduce malicious code into the BES Cyber System or introduce an unauthorized external access point to the BES Cyber System. This requirement also clarifies that these devices may be temporarily connected to the BES Cyber System, but do not become a part of the BES Cyber System, nor are they considered Protected Cyber Assets. The definition for **Transient Cyber Asset** is as follows:

A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

#	Organization	Yes or No	Question 46 Comment
46.1	WECC		Provide a separate definition of maintenance device. The requirement does not state that maintenance devices "directly connect" to BES Cyber Systems. In practice, much maintenance is done via network connections. These criteria need to be reassessed if they are intended to apply to network or remote access.
46.2	SCE&G	Agree	Are maintenance devices also to be treated as remote access, as it is a device external to the BES cyber system?26.2: TFEs may be necessary for maintenance devices not capable of supporting malicious code prevention.
46.3	Regulatory Compliance	Agree	BUT -Please clarify definition of "not permanently connected"What if you have a device that might be connected for several months?
46.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
46.5	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	Definition is good, but please see comments for questions 1.a and 1.b.
46.6	NextEra Energy Corporate Compliance	Agree	NextEra comments that if a laptop is used to remotely connect to a High Impact Control Center BES Cyber System to debug a problem or view Operator issues by temporarily gaining alarm permissions that are assigned to the Operator, is this considered a maintenance activity?
46.7	Progress Energy - Nuclear Generation	Agree	Nuclear facilities have maintenance programs based on CFR. This definition can be improved by acknowledging 10CFR50.65.
46.8	APPA Task Force	Agree	The APPA Task Force agrees with the definition.

#	Organization	Yes or No	Question 46 Comment
46.9	GTC & GSOC	Agree	We recommend the last sentence in this definition (“Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System”) be removed from R.26 and instead be included as part of the BES Cyber System definition, as suggested in our comment to 1.b. above.
46.10	Consultant	Disagree	"Examples of maintenance activities for BES Cyber Systems include configuration changes, vulnerability assessments, and software patches." NONE of these activities are maintenance activities.Configuration changes & software patches are changes covered by change control. Vulnerability assessments are tests covered by vulnerability assessments."Devices that are used for maintenance activities that are not permanently connected to BES Cyber Systems are not considered part of a BES Cyber System." This is not a definition of "Maintenance". This is (or should be) part of the definition of BES Cyber System Component. Suggest both of these statements be removed from the "definition".
46.11	Dairyland Power Cooperative	Disagree	26.2 A definition of a maintenance device seems needed here. I’m presuming this typically would be the computer used by the support staff to access the BES system for maintenance. What if maintenance is being directly performed on a BES system, is there no maintenance device involved in that case?
46.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
46.13	Network & Security Technologies Inc	Disagree	Definition is good overall but should address the question of whether a maintenance device is “external” and must therefore connect via an access point.
46.14	National Grid	Disagree	Does testing the capabilities of the relays part of the maintenance activities?
46.15	Dominion Resources Services, Inc.	Disagree	Dominion recommends revising the definition of Maintenance as follows:”Maintenance for the purpose of this standard includes any activity requiring the temporary connection of digital equipment (e.g., laptops) capable of altering the

#	Organization	Yes or No	Question 46 Comment
			configuration of, or introducing malicious code, to the BES Cyber System.”
46.16	MidAmerican Energy Company	Disagree	MidAmerican Energy agrees with EEI's comment below:The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.17	Black Hills Corporation	Disagree	Middle sentence of Maintenance definition should add ... include but are not limited to configuration...
46.18	Minnesota Power	Disagree	Minnesota Power recommends that the following definitions be adopted by the Standards Drafting Team:Maintenance: Maintenance, for the purpose of this standard, is defined as activities associated with the support, testing and upkeep of a BES Cyber System. Maintenance Equipment: Maintenance Equipment, for the purpose of this standard, is defined as any programmable, electronic device used for maintenance activities that are not permanently connected to the BES Cyber System(s). These devices are not considered part of the BES Cyber System(s).
46.19	PacifiCorp	Disagree	PacifiCorp agrees with EEI's comment below:The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.20	Southwest Power Pool Regional Entity	Disagree	Programmable, general purpose devices connected temporarily are a potentially high risk to the BES Cyber System and should have some minimum set of applicable requirements to minimize that risk. An example is the “wandering laptop” that the support staff uses to connect to High impact BES Cyber Systems and also to surf the Internet from a home Internet connection.
46.21	Duke Energy	Disagree	Suggest replacing “Cyber System Maintenance” with “Cyber System Configuration Management”. The definition (first sentence) states: "Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of a BES Cyber System." There are numerous activities that are associated

#	Organization	Yes or No	Question 46 Comment
			with support, testing, and upkeep of a BES Cyber System that are not related to cyber. This could be tuning, calibrating, etc. and could be done with a screwdriver and a meter. The second sentence includes configuration changes, vulnerability assessments, and software patches. These items are more applicable to the cyber related definition. The suggestion is to combine these sentences:"Maintenance for the purpose of this standard includes the cyber security related activities associated with the support, testing and upkeep of a BES Cyber System, including configuration changes, vulnerability assessments, and software patches."Also, please clarify if non-portable test systems that are connected to BES Cyber Systems thru an access point are included. Otherwise define “permanently connected.”
46.22	BGE	Disagree	Systems used for maintenance should be protected and sanitized per 25.1.
46.23	FirstEnergy Corporation	Disagree	The definition does not clearly specify that the intention is for temporary direct connections.
46.24	Allegheny Energy Supply	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.25	Allegheny Power	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.26	EEI	Disagree	The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.27	Southern California Edison Company	Disagree	The justification of separating end users of BES systems and those involved in maintenance is not consistent with the justification for systems that are used for maintenance. The drafting team has chosen to treat ancillary systems used to perform maintenance type activities on a BES system as equally critical. However, a distinct list of maintenance personnel is required to be maintained. The suggestion for the drafting team is to move this requirement to the section dealing with personnel.

#	Organization	Yes or No	Question 46 Comment
46.28	Progress Energy (non-Nuclear)	Disagree	Troubleshooting also needs to be explicitly included as an example.
46.29	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
46.30	We Energies	Disagree	We Energies agrees with EEI: The definition of maintenance is overbroad, and could include any number of non-electronic activities that may reasonably be performed on a BES Cyber System.
46.31	LADWP	Disagree	Will require multiple list management. Individual doing maintenance will already be on physical and electronic access list. Now another list is introduced which will also need to be maintained with the same revocation requirements. 26.1 is not necessary.

47. Requirement R26 of draft CIP-011-1 concerns procedures for BES Cyber System maintenance. Do you agree with the list of criteria that are included in Requirements Table R26? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Summary Consideration:

Commenters raised concerns about the interaction between the list of personnel in draft CIP-011-1 R26.1 and the lists of those granting authorized electronic and physical access. In addition, commenters were concerned about the interaction with other user/account management requirements. Some commenters suggested that all maintenance devices should be documented in a list. In addition, there were comments regarding the allowance for emergency maintenance situations.

Some commenters suggested that Requirement R26.1 is duplicative of Requirement R8 and should be removed, and that Requirement R26.2 is duplicative of Requirement R23 and should also be removed. The drafting team considered this feedback and has attempted to address these concerns by incorporating the requirements associated with maintenance into the requirement in CIP-007-5 – System Access Control regarding preventing the introduction of malware into the BES Cyber System, as the objective of these two requirements is the same.

#	Organization	Yes or No	Question 47 Comment
47.1	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
47.2	National Grid	Agree	Please provide clarification on 26.2.
47.3	Puget Sound Energy	Agree	Puget Sound Energy suggests additional language to clarify if personnel referenced in R26.1 are required to be maintained on the lists associated with Table 5.
47.4	Southern California Edison Company	Agree	SCE requests the Standards Drafting Team combine Requirement R26.1 with other requirements for personnel management and rationalize compliance requirements across personnel.
47.5	APPA Task Force	Agree	The APPA Task Force has no comment on this question.

#	Organization	Yes or No	Question 47 Comment
47.6	Emerson Process Management	Agree	This seems to be a typical task for properly maintaining a cyber (or computer) system. The personnel for doing this task should be already identified in the personnel training, awareness, and risk assessment. This requirement seems to be extra.
47.7	Independent Electricity System Operator	Disagree	- R26.2 define malicious code. Does malicious code mean AV or Spyware detection/prevention or does Malicious code require a code review when deploying code and patches to systems?- R26.1: suggest using a word other than “personnel”
47.8	Network & Security Technologies Inc	Disagree	26.1 - Should be reworded to distinguish “maintenance” personnel from System Administrators, who in most instances also perform maintenance activities. If the SDT concludes there is really no distinction, this requirement becomes redundant and should be eliminated, as lists of users and the permissions they have (including “System Administrator”) are already required.26.2 - Many test devices are appliances and may not be capable of meeting other CIP-011 requirements, including malicious code protection. Thus, this requirement needs to be eligible for TFEs.
47.9	Dairyland Power Cooperative	Disagree	26.1 This overlaps with the requirement of limits access based on electronic accounts. How can this be blended with user/account management?
47.10	ERCOT ISO	Disagree	26.1: Recommend addressing emergency situations more clearly. How should an entity address listing authorized personnel where support companies use a call center and cannot provide dedicated resources for the entity? This is particularly relevant for after-hours issues.
47.11	Regulatory Compliance	Disagree	26.2 - Propose this phrasing:Insure maintenance devices are free and clear of malicious code prior to the intoduction to the BES System.
47.12	Luminant	Disagree	26.2 should read "Detect and respond to the introduction of malicious code."
47.13	Southwest Power Pool	Disagree	26.2: Requirement is not necessarily applicable to special purpose testing devices, such as Fluke meters. Need to revise to limit the requirement to general purpose

#	Organization	Yes or No	Question 47 Comment
	Regional Entity		devices for which malware prevention is possible.
47.14	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
47.15	Liberty Electric Power, LLC	Disagree	CIP-026 will penalize entities if malware gets on any device, even if we employ the best available technology and processes to prevent it. This requirement needs to be removed.
47.16	Alberta Electric System Operator	Disagree	Consider revising R26.1 (or creating a new sub-requirement) to include verifying and updating the list of authorized personnel.
47.17	PacifiCorp	Disagree	Devices used for maintenance should also meet the system hardening criteria of R16 and R17.
47.18	MidAmerican Energy Company	Disagree	Devices used for maintenance should meet the system hardening criteria of R16 and R17.
47.19	Dominion Resources Services, Inc.	Disagree	Dominion appreciates the SDT's thoughts in providing this section and its associated exclusions and is very much in favor of this type of requirement. Dominion agrees with the need to protect the BES Cyber System from harm during this process, but is concerned that these requirements are overly broad.26.1. Dominion recommends that this requirement be deleted. All of these actions are covered by other requirements - access controls, change management, training (roles and responsibilities). It adds another layer of administrative paperwork to track every action made by every authorized technician with no corresponding protection to the BES. 26.2. It appears that this requirement intends to allow technicians to connect their personal laptops to relays without having to reformat them afterwards. This requirement has the unintended consequence of including any device used for maintenance (e.g., fluke meters, etc.). A footnote to avoid the necessity of a potential TFE should be added.

#	Organization	Yes or No	Question 47 Comment
47.20	US Bureau of Reclamation	Disagree	Either individuals have access authorization or they don't. This would appear to be an unnecessary tracking requirement.
47.21	RRI Energy	Disagree	Even if a maintenance device is completely up-to-date on all security patches, and also has up-to date virus detection software with the most recently release virus pattern definitions, I can not 100% ensure that malicious code will not accidentally be introduced to a BES cyber system while connected. "Ensure" is a very absolute word that is hard to match in practice. It would be better to "require " that maintenance devices have the same level of virus protection and patch management as BES Cyber Assets which the maintenance devices are being used to maintain.
47.22	ReliabilityFirst Staff	Disagree	How do personnel get authorized for addition to the list in row 26.1 and how often does this list get reviewed and updated. Add requirements for the conduct of a vulnerability assessment and actions to be taken (i.e., mitigation plan) resulting from this vulnerability assessment.
47.23	Western Area Power Administration	Disagree	How do we differentiate between "maintenance" and "administration"? This seems like a new role? This should be worked into Table R10.
47.24	WECC	Disagree	Item 26.1 would have strong impact on the ability to get timely technical support from large global companies such as Cisco Systems. Perhaps there needs to be distinct definitions for "authorized access" vs "maintenance access"? Item 26.2 seems to be covered in previous R15.The requirement does not state that maintenance devices "directly connect" to BES Cyber Systems. In practice, much maintenance is done via network connections. These criteria need to be reassessed if they are intended to apply to network or remote access.
47.25	NextEra Energy Corporate Compliance	Disagree	NextEra believes that Requirement R26 does not provide anytime frame in which the list should be reviewed nor does it take into consideration vendors. The current language does not provide clear guidance and leaves room for interpretation. The following are the recommended updates:26.1 - NextEra suggests maintaining a list of

#	Organization	Yes or No	Question 47 Comment
			personnel authorized to perform maintenance on the BES Cyber System, allow authorized personnel to escort cyber and physical vendors, and allow only authorized personnel to perform maintenance on the BES Cyber System. The list of personnel authorized to perform maintenance of the BES Cyber System should be updated at least annually.Maintenance devices not permanently connected to BES Cyber Systems are not considered part of the BES Cyber System.
47.26	Allegheny Energy Supply	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.27	Allegheny Power	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.28	EEI	Disagree	R 26.1 is duplicative of Requirement 8 and should be removedR 26.2 is duplicative of Requirement 23 and should be removed.
47.29	Southern Company	Disagree	R.26.1 If personnel are required to have a PRA, are granted physical access, system usage is logged and the individual has access credentials for cyber systems, the additional list generation should not be required.Vendor personnel supporting systems would need to be added to the personnel listing, these personnel frequently change. The addition of a name to the list would become a common event.
47.30	Consultant	Disagree	R26 - Suggest changing wording to "implement and document"Suggest changing wording to: "Systems and to ensure that" for correct grammar.R26 - Delete the word "accidentally" from the statement. It would appear a better objective is to prevent the introduction of malicious code, "accidentally" or "intentionally" is not relevant to the objective.Table R26 - Item 26.1 This is a new account management requirement. There are account management activities for cyber access, physical access, information access, and now maintenance access. As such this requirement should be moved to the account management requirements table.Item 26.2 This is not a requirement statement, it is a statement of a desired objective. It is not clear what

#	Organization	Yes or No	Question 47 Comment
			requirement or requirements are intended to meet this objective. Please clarify the requirement.
47.31	FirstEnergy Corporation	Disagree	R26 text needs to be more specific that the intention is for temporary direct connections. Otherwise, R26 appears to be covering CIP 7R1 and 7R3.
47.32	Progress Energy (non-Nuclear)	Disagree	R26.1 - do not see need for this requirement. Changes can only be made with cyber access rights which is covered by other requirements.R26.2 - either eliminate this requirement or make additional provisions for the safe use of maintenance components. CIP standards shouldn't mandate malware protection on all test equipment. The BES Cyber Systems components should already be adequately protected from threats as a result of being compliant with the other requirements.We like the use of the footnote earlier in the standard that allowed the use of the highest level of protection the components can support maybe something like that could be used here too.
47.33	Public Service Enterprise Group companies	Disagree	R26.1 requires maintaining another list of personnel who perform maintenance on a BES Cyber System. These individuals are already tracked and documented under other access lists. Seems like a duplication of effort with no benefit and thus the requirement should be deleted.
47.34	Xcel Energy	Disagree	R26.2 - The requirement should be worded to require anti-malware protection on all maintenance devices. The current wording would make it an enforceable violation if, in spite of best efforts, malware was introduced in to a device.
47.35	Hydro One	Disagree	Recommend adding a Requirement for listing the devices used for maintenance activities.
47.36	Northeast Power Coordinating Council	Disagree	Recommend adding a Requirement for listing the devices used for maintenance activities.

#	Organization	Yes or No	Question 47 Comment
47.37	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that different sections with similar requirements be aligned to avoid confusion. In Table 26, with respect to R26.1, other sections contain similar requirements for Physical Security, Electronic Access, and System Security. We'd prefer to see them re-aligned in a fashion similar to the way the older version of the Standards have them. The new maintenance requirements can be added into those Standards. Similar comment for 26.2; SDG&E feels that this could have been added to the System Security/Protection area.
47.38	LADWP	Disagree	See previous
47.39	BGE	Disagree	Should not have a separate list for maintenance personnel. All personnel should be included on the access control lists created per R7 - R14.
47.40	Duke Energy	Disagree	Suggest replacing "Cyber System Maintenance" with "Cyber System Configuration Management".Requirement 26.1: Please consider adding the word "cyber security related" to make the definition read as follows:Maintain a list of personnel authorized to perform cyber security related maintenance on the BES Cyber System and allow only authorized personnel to perform maintenance on the BES Cyber System.Requirement 26.2: Please consider changing as highlighted below:Detect and prevent the introduction and propagation of malicious code on all computer based maintenance devices.Remove 'accidently' from R26. Suggest removing all of R26.26.1 Specify maintenance performed is done with the maintenance device. We interpret 26.1 to be that the maintenance personnel would not have to be background screened and trained. Suggest including screens and trains for these folks. Or remove the requirement with the understanding that these personnel will have electronic or unescorted physical access to the BES Cyber System. This is extra work for no added security.26.2 will need a TFE. Within generation, we have differing opinions on the definition of code. Suggest clarifying that it does not include programming code.
47.41	Detroit Edison	Disagree	Table R26.2 only addresses the introduction and propagation of malicious code into

#	Organization	Yes or No	Question 47 Comment
			the BES Cyber System. It is likely however, that a device may be modified not to introduce or propagate code but act as a bridge to another rogue network via wireless, cellular or other medium. This would be akin to introducing an unsecured access point into the boundary if this system is not subject to the same requirements equal to or greater than that of highest impact BES Cyber System component. A possible solution could be to require mitigation for multi-homed or bridged networks for all components used for BES Cyber System maintenance, and/or append R26 to read "...and ensure that systems used for maintenance do not introduce malicious code into the BES Cyber System or act as an unauthorized access point into an Electronic Security Perimeter."
47.42	Bonneville Power Administration	Disagree	The objective of this requirement ("to prevent unauthorized maintenance on BES Cyber Systems and ensure that systems used for maintenance do not accidentally introduce malicious code into the BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R26, Section 26.2. It is impossible to prevent the introduction and propagation of malware. This is already addressed in Requirement 15. Recommendation: Delete Section 26.2.
47.43	Manitoba Hydro	Disagree	The personnel authorized to perform maintenance on the BES Cyber System should be identified by roles, not individual names. There are no specifics given with respect to "prevent" in Requirement R26.2 so it is assumed to be at the Responsible Entity's discretion in terms of means, criteria, etc.
47.44	Reliability & Compliance Group	Disagree	There is a possible issue that could occur with this requirement regarding collective bargaining unit rules. It may require that job classifications be created for individuals who work on these systems.

#	Organization	Yes or No	Question 47 Comment
47.45	Constellation Energy Commodities Group Inc.	Disagree	There is no definition of malicious code provided. Clarify the scope of malicious code to include virus, malware and spyware protection, as currently generally commercially understood.
47.46	Minnesota Power	Disagree	Using the definitions proposed in Question 46, Minnesota Power recommends that Requirement R26 state that "prior to connecting Maintenance Equipment or importing data, patches, code or other electronic files into the BES Cyber System, the device and/or files shall be scanned for malware and up-to-date on security patches."
47.47	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
47.48	We Energies	Disagree	We Energies agrees with EEI: R 26.1 is duplicative of Requirement 8 and should be removedWe Energies agrees with EEI: R 26.2 is duplicative of Requirement 23 and should be removed.
47.49	Florida Municipal Power Agency	Disagree	Why is malware mentioned in 26.2, when it already has been covered in R15? FMPA believes this should be removed.

48. Table R26 provides direction concerning what impact level of BES Cyber Systems to which Requirement R26 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Several commenters suggested that the types of connectivity used for temporary connections should be considered. In addition, several commenters suggested that the criteria should be applied to all impact levels. There was also a comment for a no impact category.

The drafting team considered this feedback and attempted to address these concerns by incorporating the requirements associated with maintenance activity into the requirement in CIP-007-5 – System Access Control regarding preventing the introduction of malware into the BES Cyber System, as the objective of these two requirements is the same.

#	Organization	Yes or No	Question 48 Comment
48.1	WECC		Criteria should apply to all impact levels
48.2	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R26 if it is understood that a blank in the table means N/A.
48.3	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
48.4	Progress Energy - Nuclear Generation	Agree	R26 can be improved by incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments.
48.5	Allegheny Energy Supply	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extend an electronic security perimeter.

#	Organization	Yes or No	Question 48 Comment
48.6	Allegheny Power	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extend an electronic security perimeter.
48.7	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
48.8	American Municipal Power	Disagree	Please provide a little or no impact category
48.9	BGE	Disagree	Should not be separate requirements for maintenance of BES Cyber Systems.All personnel should be included on the access control lists created per R7 - R14.
48.10	Consultant	Disagree	The comments on Question 47 regarding moving item 26.1 elsewhere, and Item 26.2 not being a requirement statement preclude an evaluation of application to impact categories.
48.11	Duke Energy	Disagree	Require for low when the maintenance device also connects to medium or high systems.
48.12	EEI	Disagree	R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extent an electronic security perimeter.
48.13	Entergy	Disagree	Basic Maintenance requirements should apply equally for all components of a control system
48.14	FirstEnergy Corporation	Disagree	Until clarity is provided on the above comments (Q46 and Q47), we can not provide a

#	Organization	Yes or No	Question 48 Comment
			response to this question.
48.15	Florida Municipal Power Agency	Disagree	FMPA believes this standard should be removed entirely, as it is already addressed under account control, R7.
48.16	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
48.17	Progress Energy (non-Nuclear)	Disagree	See comment 14.
48.18	Public Service Enterprise Group companies	Disagree	General agreement, but Requirement 26.2 may not be technically feasible for certain types of maintenance devices. To implement this requirement, an Operating System level change to the component may be required, which may be infeasible or not available from the Original Equipment Manufacturer (OEM). This requirement needs to be qualified with the phrase "where technically feasible".
48.19	ReliabilityFirst Staff	Disagree	Suggest "Required" for Low Impact in rows 26.1 and 26.2.
48.20	San Diego Gas and Electric Co.	Disagree	SDG&E suggests that different sections with similar requirements be aligned to avoid confusion. In Table 26, with respect to R26.1, other sections contain similar requirements for Physical Security, Electronic Access, and System Security. We'd prefer to see them re-aligned in a fashion similar to the way the older version of the Standards have them. The new maintenance requirements can be added into those Standards. Similar comment for 26.2; SDG&E feels that this could have been added to the System Security/Protection area.
48.21	Southern California Edison Company	Disagree	The drafting team has chosen to treat ancillary systems used to perform maintenance type activities on a BES system as equally critical. If this is not the intent of the team, the wording of the standard should be modified to reflect the difference in impact levels.

#	Organization	Yes or No	Question 48 Comment
48.22	Southwest Power Pool Regional Entity	Disagree	26.2 should be applicable to all impact categories.
48.23	US Army Corps of Engineers, Omaha Distirc	Disagree	There needs to be a provision for emergency work. Whether that means talking someone through a fix at 2am or hiring a vendor for additional expertise.
48.24	We Energies	Disagree	We Energies agrees with EEI: R26 is problematic as it does not effectively address the different possible methods that may be used to perform 'Maintenance'. For example a configuration change may be made to certain equipment using a serial cable between a BES Cyber System and a technician craft terminal. This does not create or extent an electronic security perimeter.

49. Requirements R27 to R29 of draft CIP-011-1 concern procedures for Cyber Security Incident response. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R27 to R29? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Cyber Security Incident Response" is now addressed in CIP–008–5 — Cyber Security — Incident Reporting and Response Planning.

One of the primary focus areas of the comments concerned coordination with the reporting requirements in CIP 001 and EOP-004 for reporting to the ES-ISAC, and additional guidance in determining incident classifications. The SDT has attempted to coordinate with the drafting team working on revisions to CIP-001 and EOP-004 to ensure the two sets of requirements are coordinated. As the two teams are working in parallel, continued coordination will be necessary.

Several commenters asked for definitions for cyber security incidents and reportable cyber security incidents. The SDT developed a revised definition for "**BES Cyber Security Incident**" as follows:

A malicious act or suspicious event that:

- *Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or*
- *Results in unauthorized physical access into a Defined Physical Boundary.*

The SDT also proposed a new definition of "**Reportable Cyber Security Incident**" as follows:

Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service.

Several requests were made to clarify the periodic timing requirements such as annual, calendar year, and 12 months. The drafting team reviewed the timing elements of all requirements and where there was a reference to "annual" the SDT replaced this with the following:

". . . at least once each calendar year, not to exceed 15 calendar months between. . ."

Some commenters recommended placing all requirements in the table, not in the objective or in the "pre-amble" for cyber incident reporting, and the drafting team has included all mandatory performance in the requirements.

Many commenters requested clarifications for plan testing requirements, operational exercises, test environment, as well as the number of tests required. The drafting team did attempt to add more clarity to plan testing requirements along with operational exercise, test environment, and number of tests required in the revised standard (CIP-008-5).

Guidance was requested regarding review of the results of incident response tests in less than 60 days. The revised standard now requires the review to take place within 30 calendar days and the update, based on lessons learned, to take place within 60 calendar days of the test.

Some commenters asked for clarity on the inclusion of physical breach aspects of cyber security incidents as reportable. The drafting team is coordinating its revisions with the revisions to CIP-001 and EOP-004 underway through Project 2009-01 – Disturbance and Sabotage Reporting.

There were concerns raised as neither logging nor monitoring are required for Low Impact BES Cyber Systems, there is no basis for requiring Cyber Security Incidents on these systems to be tracked or classified. The applicability section of the entire suite of CIP Version 5 standards has been revised to provide greater clarity on which BES Cyber Systems (High, Medium, and Low Impact) are applicable to specific requirements.

#	Organization	Yes or No	Question 49 Comment
49.1	National Rural Electric Cooperative Association (NRECA)		In R27.1 a "process" is required, but it is not clear as to how a utility is required to "classify" events. Please provide further clarification as to how one is required to "classify" these events.In R29.1 the requirement is to review the plan once every 12 months. Please provide specificity as to what "once every 12 months" means. If I review the plan on Jan. 15, 2001, am I in compliance if I review it again by Jan. 25, 2002? Please make sure that this is clear in the requirement and in all requirements of CIP-010-1 and CIP-011-1.
49.2	Tenaska		Consider combining 28 and 29
49.3	Black Hills Corporation	Agree	Request that the language in 27.3 be broadened to include contacting appropriate law enforcement authorities, similar to CIP-001.
49.4	FEUS	Agree	Agree with Comments: the drafting should clarify the reporting time requirement for

#	Organization	Yes or No	Question 49 Comment
			27.3, reporting to the ES-ISAC
49.5	Green Country Energy	Agree	I really see the need for a reference document or footnotes pointing to sources for guidance on the expectations for these requirements.
49.6	SCE&G	Agree	R29 is a good example of an instance where there are a lot of timing requirements embedded in the requirements. It would be helpful to entities if timing requirements were consistently put in the same location in the tables (under the low, medium, and/or high columns) rather than embedded in the text. The SDT should evaluate the number of timed requirements in relation to the low, medium, and high impact categories. Once the requirements are finalized it would be of benefit to entities to have a list of the timeframe type requirements which must be met for each low, med, and high impact system, as these often present some of the greatest administrative burden in documenting these timeframes were met.
49.7	Allegheny Energy Supply	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.
49.8	Allegheny Power	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.
49.9	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
49.10	Ameren	Disagree	R27 would be better suited in CIP-001, Sabotage Reporting.â€,â€,â€,

#	Organization	Yes or No	Question 49 Comment
49.11	American Electric Power	Disagree	27.1 - 27.3: Recommend requiring this for systems with routable external connectivity only. To properly monitor and alert on cyber security events, a trained IT Security Operations staff and dedicated set of monitoring tools are required. If there is no external connectivity, there is no access for the IT teams to monitor these cyber systems.
49.12	APPA Task Force	Disagree	The APPA Task Force supports the drafting team's efforts on incident response. We propose the following edits:The APPA Task Force believes that NERC, as the ES-ISAC, should have a standard process for entities to use in reporting Cyber Security Incidents. Therefore, we propose the following wording for R27 Table 27.3: 27.3: Use the reporting guidance developed by the ES-ISAC for reporting Cyber Security Incidents, either directly or through an intermediary, or develop a process equivalent or superior to that guidance.28.1, recommend changing "once every 12 months" to "Annually."29.1, recommend changing "once every 12 months" to "Annually."
49.13	Bonneville Power Administration	Disagree	The objectives of these requirements ("so that responses to Cyber Security Incidents involving BES Cyber Systems can occur" and "to verify its response plan's effectiveness in responding to a Cyber Security Incident impacting a BES Cyber System") should be clearly labeled as "Objective of Requirement" and shown as a separate sentence prior to the text of the requirement rather than appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table 28, Section 28.1. It's not clear whether testing in January 2010 and June 2011 would satisfy the requirement, since February 2010 through January 2011 would be a 12-month period with no testing. Recommendation: Replace "every 12 months" with "each calendar year". Also, there are other ways to test, as well. Recommendation: "Test the execution of the incident response plan (by recovering from an actual incident, or with a test at least as comprehensive as a paper drill) at ... Table 29, Section 29.1. Same comment as 28.1

#	Organization	Yes or No	Question 49 Comment
49.14	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
49.15	Consultant	Disagree	R27 - "...so that responses to Cyber Security Incidents involving BES Cyber Systems can occur." should be reworded. Suggest "to identify responsibilities and actions in response to an incident associated with BES Cyber Systems."Table R27 - should specify in each statement that it applies to BES Cyber Systems."Cyber Security Incident" is defined in the Glossary using the terminology from CIP-002 through CIP-009. That definition should be revised by including a new definition in this standard using the terminology associated with CIP-010 and CIP-011.Item 27.3 Not all Cyber Security Incidents are reportable to ES-ISAC as indicated in The Security Guidelines for the Electricity Sector: Threat and Incident Reporting, version 2.0, dated April 1, 2008. Suggest clarifying the statement about reporting.Table R28 - Item 28.1 Clarify the periodicity to be consistent throughout the standard. Annual, 12 months, or other statement. Suggest getting information from the nuclear industry on stating and handling periodicity of requirements.Table R28 - Item 28.1 It is not clear from the table whether one test is required, or two tests (one for High Impact & one for Medium Impact) Suggest some clarification wording in the requirement statement.Table R29 - Item 29.1 Clarify the periodicity to be consistent throughout the standard. Annual, 12 months, or other statement. Suggest getting information from the nuclear industry on stating and handling periodicity of requirements.Item 29.2 - Suggest deleting the word "each" as an unnecessary word.Item 29.3 - Actions necessary to address documented plan deficiencies may not be completed within 30 days, so requiring an update to the plan with 30 days would appear to create a situation where compliance is not viable, or sensible. Suggest modifying to be based on completion of corrective actions.Item 29.5 Suggest deleting the word "all" as an unnecessary word.
49.16	Detroit Edison	Disagree	Table 28.1 and 29.1 refer to a period of "12 months". We prefer “at least once per calendar year, not to exceed 14 months between instances”.

#	Organization	Yes or No	Question 49 Comment
49.17	Dominion Resources Services, Inc.	Disagree	Per R18, neither logging or monitoring are required for Low Impact Systems, hence there is no basis for requiring Cyber Security Incidents on these systems to be tracked or classified.
49.18	Duke Energy	Disagree	Requirement 27: The requirements need a definition of a "Cyber Security Incident". This needs to differentiate between a cyber security attack and a mistake that a technician makes in the plant. We don't need to report every time a technician forgets their password.Requirement 28 only has one item and it is related to Requirement 29. Perhaps combine these two?Table 28: 28.1 assumes there is only one incident response plan when R27 allows for multiple plans. We would like to test AN incident response plan instead of all of them. Or allow for a different time frame (12 months per plan) to test all of them. Combine 28 with 29 if the VSL is the same.Table 29: 29.1 We would like to review AN incident response plan instead of all of them. Or allow for a different time frame (12 months per plan) to review all of them.
49.19	E.ON U.S.	Disagree	Comments: CIP-011, R27 The application of this standard to low-impact BES CS's seems inconsistent. There are not requirements for monitoring security events associated with these assets.CIP-011, R29.1 The application of this standard to low-impact BES CS's seems inconsistent with other requirements for monitoring security events associated with these assets.CIP-011, R30.2 Please clarify whether "...identification of the personnel responsible..." require naming individuals, or job functions?
49.20	EEI	Disagree	Suggested modification to R27.3: "Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC)."If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.

#	Organization	Yes or No	Question 49 Comment
49.21	Emerson Process Management	Disagree	Without being required to perform tasks in System Security, low impact BES Cyber systems may not be able to easily classify cyber security incidents.
49.22	Entergy	Disagree	The current definition of “Cyber Security Incident” will need to be changed as it references ESPs and PSPs. As such, it may be a good idea to define what this term means here.It is observed that as written there is no longer a requirement to keep documentation associated with a Cyber Security Incident (i.e., akin to CIP-008 R2). Is this the intent?
49.23	ERCOT ISO	Disagree	29.2: Should be 30 days rather than 60 days to align with FERC Order 706.
49.24	FirstEnergy Corporation	Disagree	27.1: From CIP-008 R1.1, what happened to the concept of "reportable"?
49.25	Independent Electricity System Operator	Disagree	- R27.1: note that the word “reportable” has been removed; CIP-008-2, R1.1 stated “Procedures to characterize and classify events as reportable Cyber Security Incidents”- R28.1: modify the sentence to state “Test the execution of the Cyber Sec
49.26	ISO New England Inc	Disagree	see recommendation for review in prior requirements use same for all annual/ 12 month review.
49.27	Manitoba Hydro	Disagree	The wording of Requirement R28.1 should be revised as the phrase “with a paper drill” could be misinterpreted. There are no specifics given with respect to ‘classifying’ events in 27.1 so it is assumed to be at the Responsible Entity’s discretion in terms of criteria, etc.
49.28	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R27, but recommends that the last phrase be changed from “so that responses to Cyber Security Incidents involving BES Cyber Systems can occur” to “so that responses to Cyber Security Incidents involving BES Cyber Systems follow a defined plan.” Responses can (and will) happen with or without a plan. The purpose of R27 is to define, ahead of time, a process to ensure an orderly response.Minnesota Power

#	Organization	Yes or No	Question 49 Comment
			generally agrees with the proposed Requirements R29, but recommends that this Requirement should be revised to ensure consistency with Requirement R32. For example, Part 29.1 should state "Review the incident response plan(s) at least once every 12 months or when BES Cyber System(s) have any system, organization or technological changes. Document any identified deficiencies, changes or improvements.") If this language was consistent with Requirement R32, the following issues could be resolved. In addition, the Standards Drafting Team should consider whether or not Parts 29.2 - 29.5 should also be required of Medium Impact Systems (since Part 28.1 requires testing for those systems) with a longer timeframe.
49.29	Network & Security Technologies Inc	Disagree	R27 - should clarify whether cyber security incidents of a physical nature are included and, if so, should tie back to 5.11.29.2 - Sixty days seems like a very long time to wait before evaluating the effectiveness of response actions, esp. if they were taken in response to an actual incident. Suggest revising to require a much more immediate "after action" review, at least for actual incidents. Should be a matter of days - perhaps 7 or less, not months. Even for tests, 60 days seems overly generous. Suggest revising to 30 days.
49.30	Nuclear Energy Institute	Disagree	Does the definition of cyber security incident, as used in this Standard, comport with the definition in Section 215 of the FPA? ("The term "cybersecurity incident" means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system.")
49.31	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
49.32	Progress Energy - Nuclear Generation	Disagree	Incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security

#	Organization	Yes or No	Question 49 Comment
			Plans for comments for nuclear generating facilities.
49.33	Progress Energy (non-Nuclear)	Disagree	What makes 28.1 and 29.1 different that requires 2 different requirements? If you test the execution every 12 months then you have effectively done a review.
49.34	ReliabilityFirst Staff	Disagree	Problem with auditing the "effectiveness" of R28 without some clear guidelines that would lead to consistent application by all auditors. For R29.4, please clarify what is meant by system, organizational, and technology changes.
49.35	San Diego Gas and Electric Co.	Disagree	SDG&E believes that the Incident Response Plan requirements should only apply to Medium and High impact assets. Including Low impact assets in these requirements seems like overkill. For example, in R27.3, we don't feel that we would necessarily report a "Cyber security incident" on a Low impact item to ES-ISAC.
49.36	Southwest Power Pool Regional Entity	Disagree	27.1: Should be a "reportable" cyber incident. May be appropriate to add as a separate requirement to identify Cyber Security Incidents as "reportable." 27.2: "Communication plans" needs to be defined somewhere. 28.1: Consider changing "Test the execution of the incident response plan" to "Exercise the incident response plan." Clarify that the exercise scenario must involve a covered BES Cyber System and that the exercise must follow (actually exercise) the incident response plan steps. Also need to clarify whether each BES Cyber System, or at least one in each impact category represented, must be included in the exercise. Requiring the inclusion of each BES Cyber System is not recommended due the potential burden; this is a clarification issue to ensure the entities and the auditors have the same understanding. 29.1: Should the 12-month requirement be +/- one month? 29.2: Reviewing an exercise or actual response 60 days after the fact is too long. To keep it fresh in the minds of the responders, 30 days max is suggested, 15 days for High impacting systems is preferred.
49.37	US Bureau of Reclamation	Disagree	Why would we have incident reporting requirements related to systems that we have no processes to track them on...? This would appear to be in conflict with many of

#	Organization	Yes or No	Question 49 Comment
			the previous requirements that did not apply to low systems.
49.38	We Energies	Disagree	We Energies agrees with EEI: Suggested modification to R27.3: “Process for providing reports of Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).”We Energies agrees with EEI: If Cyber Security Incidents are different than sabotage reports as required in CIP-001, then they need to be defined. If they are the same as required in CIP-001, then R27.3 should be deleted.

50. Tables R27 to R29 provide direction concerning what impact level of BES Cyber Systems to which Requirements R27 to R29 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Cyber Security Incident Response" is now addressed in CIP–008–5 — Cyber Security — Incident Reporting and Response Planning, and "Cyber Security Incident Response Plan Testing" is addressed in CIP-009-5 - Cyber Security — Recovery Plans for BES Cyber Assets and Systems."

The primary focus areas of the comments received was on impact levels and the concern for coordination with the reporting requirements in CIP 001. The SDT has coordinated with the drafting team working on revisions to CIP-001 to ensure the two sets of requirements are coordinated.

Many commenters requested that Incident Response requirements for Low Impact BES Cyber Assets or non-routable connections be removed along with providing improved consistency between requirements related to impact level. The revised requirements (now contained in CIP-008-5) do not apply to Low Impact BES Cyber Assets. The SDT updated the applicability section of all requirements in the entire suite of CIP Version 5 standards.

It was suggested that Requirement R28.1 should be modified to clarify that test plans should be exercised once each calendar year (vs. every 12 months), and that these tests will be conducted on an overall system basis and not on a per system or per component level basis. This requirement is defined in CIP-009-5 Requirement R2.1, Recovery Plan Implementation and Testing. There were suggestions regarding the clarification of the plan testing requirements, operational exercises, and test environment, and there were comments regarding the addition of guidance on Cyber Security Incident classification by adding glossary definitions of Cyber Security Incident and Reportable Cyber Security Incident. The testing requirements, operational exercises, and test environment are described in CIP-009-5, and a couple of terms were added to the NERC Glossary for completeness.

The SDT developed a revised definition for "**BES Cyber Security Incident**" as follows:

"*A malicious act or suspicious event that:*

- *Compromises, or was an attempt to compromise, the Electronic Security Perimeter, or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or*
- *Results in unauthorized physical access into a Defined Physical Boundary."*

The drafting team proposed a new definition of "**Reportable Cyber Security Incident**" as follows:

" Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service."

A few comments were directed at reviewing of results of Incident Response tests in less than 60 days, including the physical aspects of Cyber Security Incidents. The SDT modified this requirement and now requires that this review be performed within 30 days of the BES Cyber Security incident or test and to update the BES Cyber System Incident response plan based on lessons learned within 60 calendar days of the BES Cyber Security incident or test.

Issues identified in comments for the SDT to consider for modifications included additional guidance on performing Cyber Security Incident classification. This is now covered in the guidance documentation for CIP-008 and CIP-009..

With Version 5, the drafting team has worked to make the applicability for each requirement very clear.

#	Organization	Yes or No	Question 50 Comment
50.1	Hydro One		Recommend for consistency incident response plan for medium and high impact mirrors 31.1 and 31.2 time frames not to exceed 24 and 12 months respectively.
50.2	APPA Task Force	Agree	The APPA Task Force agrees with the impact levels proposed for R27-R29 if it is understood that a blank in the table means N/A.
50.3	Bonneville Power Administration	Agree	Items 28.1 in Table R28 and 29.1 in Table R29 states that the incident response plan shall be tested "at least once every 12 months" and that the incident response plan should be reviewed at least once every 12 months." Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently testing or review must occur.
50.4	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
50.5	Florida Municipal Power	Agree	FMPA believes "12 months" should be changed to "annual"

#	Organization	Yes or No	Question 50 Comment
	Agency		
50.6	PacifiCorp	Agree	29.3 - Does the requirement to update each response plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?29.4 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the response strategy or response activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the response.
50.7	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	Agree	See comment for question 6.
50.8	Southern California Edison Company	Agree	SCE recommends that the standards drafting team use the phrase “cyber security incident” or “physical security incident” to differentiate them from the occurrence of system events that may or may not result from the breach of a “cyber” or “physical” control. As the Requirements are currently written, there is no logging and monitoring requirements for low impact systems. It is inconceivable how a registered entity could implement an incident response plan at these facilities when per CIP standards access and use of these facilities is not required. If the drafting team intends for incident response, as it pertains to Sabotage Reporting under CIP 001, they should state it.
50.9	Alberta Electric System Operator	Disagree	In Table R29, for 29.2, consider revising to review results for High Impact systems to within 30 days, and Medium Impact systems to within 60 days.
50.10	Allegheny Energy Supply	Disagree	R 28.1 should be modified to be clear that testing of incident response plans need not

#	Organization	Yes or No	Question 50 Comment
			include every possible BES Cyber System.
50.11	Allegheny Power	Disagree	R 28.1 should be modified to be clear that testing of incident response plans need not include every possible BES Cyber System.
50.12	Alliant Energy	Disagree	Alliant Energy agrees with the EEI Comments
50.13	Ameren	Disagree	R28.1 - Based on the number of Medium Impact Systems this will be labor intensive with no added protection to the BES. Suggest that this requirement only remain for High Impact Systems.
50.14	American Electric Power	Disagree	Please see response to Question 49.
50.15	American Municipal Power	Disagree	Please provide a little or no impact category
50.16	American Transmission Company	Disagree	R27 requires a response to cyber security incident for all Low Impact BES Cyber Systems; however R18 does not require monitoring and/or logging of Low Impact BES Cyber Systems. How do you respond to an incident unless it is being monitored?
50.17	BGE	Disagree	R29 should apply to any BES Cyber System required in R28.
50.18	Black Hills Corporation	Disagree	28.1 and 29.2 should also be required for Low Impact BES Cyber Systems.
50.19	Consultant	Disagree	Table R27 to Table R29 - It doesn't appear to make sense that the Incident Response Plan applies to all impact level categorizations, while testing the plan applies to Medium Impact & High Impact assets, and actions related to updating the plan only apply to High Impact assets.It would seem logical that the columns in this table should indicate the requirements apply to the same impact level assets, which would be either only High Impact assets, or Medium & High Impact assets, but not a mix.
50.20	Dominion Resources	Disagree	29.2 - 29.5 should be required for Medium Impact to be consistent with R28. R29.2 thru R29.5 currently use text to convey numbers (e.g., sixty vs. 60). This is not

#	Organization	Yes or No	Question 50 Comment
	Services, Inc.		consistent with the convention used throughout CIP-011 and is more difficult to read. A single convention using numerical values should be used throughout.
50.21	Duke Energy	Disagree	Requirement 28.1: is this one test of the cyber incident response plan (global) once per 12 months or is this the test of test of the cyber incident response plan for EACH BES cyber system per 12 months? Once globally per 12 months should be plenty.Requirement 29.5: is the communication of updates a broadcast or is specific feedback from each person required? Remove these requirements for Low Impact.
50.22	EEI	Disagree	EEI suggest that R 28.1 should be modified to be clear that test plans should be exercised annually and not at a per system or per component level.
50.23	Entergy	Disagree	These Requirements should apply for all three BES Cyber System/Component Impact categories.
50.24	Garland Power and Light	Disagree	Requirement 27.1, 27.2, 27.3 and 29.1 - remove from “Low Impact” classification
50.25	ISO New England Inc	Disagree	If the Entity’s Incident Response Plan is tested (instead of testing each BES Cyber System), recommend that “Require” should apply for High Impact, Medium Impact, and Low Impact BES Cyber Systems
50.26	LADWP	Disagree	Table 27 - low impact should not be included.
50.27	Manitoba Hydro	Disagree	Cyber Security Incidents for Low Impact BES Cyber System should not require reporting to the ES-ISAC.
50.28	MidAmerican Energy Company	Disagree	29.3 - Does the requirement to update each response plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency? 29.4 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is

#	Organization	Yes or No	Question 50 Comment
			considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the response strategy or response activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the response.
50.29	Minnesota Power	Disagree	With the implementation of the changes discussed in Question 49, these impact levels are generally acceptable.
50.30	National Grid	Disagree	o National Grid recommends deleting 27.3 for Low Impact BES CS o National Grid recommends the timeframes for Medium and High Impact in R28 similar to Table R31 31.1 and 31.2 for consistency.
50.31	Network & Security Technologies Inc	Disagree	Table 27 includes Low Impact systems, but Table 18 (event monitoring) does not. Need to change one or the other.
50.32	Northeast Power Coordinating Council	Disagree	Recommend for consistency incident response plan for medium and high impact mirrors 31.1 and 31.2 time frames not to exceed 24 and 12 months respectively.
50.33	Oncor Electric Delivery LLC	Disagree	The Incident Response Plan should be required for the entity, not for every High Impact cyber system. Requirement 29.4, update of Incident Response Plan, we suggest these reviews be conducted quarterly.
50.34	Pepco Holdings, Inc. - Affiliates	Disagree	We agree with EEI's comments.
50.35	Progress Energy (non-Nuclear)	Disagree	Need to clarify the annual/12 month/365 day issue.
50.36	ReliabilityFirst Staff	Disagree	For R29, each subrequirement should be "Required" for all the "Medium" impact BES Cyber Systems.

#	Organization	Yes or No	Question 50 Comment
50.37	San Diego Gas and Electric Co.	Disagree	SDG&E also feels that instead of using the word “impact” for these Requirements, apply a concept of “risk” for inclusion. We would want to identify the risks with associated systems security and protect accordingly
50.38	Southwest Power Pool Regional Entity	Disagree	28.1 should be applicable to all impact categories. An incident response plan should be tested to verify that it will work when needed. 29.2 through 29.5 should be applicable to all impact categories, perhaps with shorter time frame for higher impact systems.
50.39	US Bureau of Reclamation	Disagree	Why would we have incident reporting requirements related to systems that we have no processes to track them on...? This would appear to be in conflict with many of the previous requirements that did not apply to low systems.
50.40	We Energies	Disagree	We Energies agrees with EEI R 28.1 should be modified to be clear that testing of incident response plans need not include every possible BES Cyber System.
50.41	WECC	Disagree	All items should be required for medium impact levels in R29Criteria should apply to all impact levels.

51. Requirements R30 to R32 of draft CIP-011-1 concern procedures for BES Cyber System Recovery. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R30 to R32? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Summary Consideration:

Note that "Recovery Plans" are now addressed in CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems

The primary focus areas of the comments were concerns with improving the clarity of the periodic timing requirements, the requirement to reinstall and configure any application and system software using its baseline configuration vs. functionality, and the recognition that a large amount of test equipment will be necessary to develop representative environments for numerous disparate facilities.

Some commenters noted the different terms used for references to annual activities. The SDT reviewed the use of annual, calendar year, 12 months, etc. and in the revised standards used the phrase, ". . .at least once each calendar year, not to exceed 15 calendar months between. . ." .

There were suggestions that the testing requirements should only apply to control centers. Additional guidance was requested for operational testing, the use of redundant sites as an acceptable means to address recovery, and for testing of information that is stored on backup media. The SDT added some information about testing in the Rational Box for the proposed CIP-009-5 R1. Testing is necessary to verify the Responsible Entity's Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

Recovery Testing – Operational Test every 36 months should count for the annual test. The SDT notes that there is a FERC directive to add a requirement to conduct a full operational test of the recovery plan once every three years – so the suggestion to count the full operational test as the annual test was adopted. Areas of opportunity suggested for modification of the standards by the SDT were to provide recovery plan testing clarifications, data retention plan clarification, identification requirements of "Personnel Responsible", and incident recovery plan reviews.

Commenters suggested changes and provided various requests/suggestions for re-wording/wordsmithing and improved coordination of backup and recovery with EOP-008. The SDT has coordinated its proposed requirements with the now FERC approved EOP-008-1 – Loss of Control Center Functionality. Commenters suggested that all requirements should be in the table, not in the objective or in the "pre-amble" to the requirements and that the SDT should consider providing a summary table for all periodic requirements and remove the "how to" statements from the requirements. The SDT has included all mandatory performance in the requirements of the revised

standards. The SDT did not adopt the suggestion to develop a summary table for periodic requirements as the format for Version 5 is considerably different from the format proposed when the requirements were all combined in CIP-011.

Several commenters suggested adding definitions for terms such as "initially stored," and the SDT believes that these terms do not have a unique meaning when used in the standard and do not require a formal definition. The team has tried to limit its proposed definitions to those terms that either have a unique meaning when used in a NERC Reliability Standard, or when misunderstanding a word may have a material impact to reliability.

#	Organization	Yes or No	Question 51 Comment
51.1	Dairyland Power Cooperative		30.5 does the system test require a test of every element in the recovery plan? If a recovery plan covers multiple systems, must all systems be tested annually? Or is it sufficient to test some scenarios affecting some systems?
51.2	National Rural Electric Cooperative Association (NRECA)		In R31.1 and R31.2 there are references to "once every 24 months" and "once every 12 months." Please ensure these timeline requirements are clear similar to my comments in Question 49 regarding R29.1.
51.3	SCE&G		R31.3: What constitutes and operational exercise? What is the scope of the recovery and systems to be covered (all high impact cyber systems, or one sample system if the same recovery plan is used acroos all)?
51.4	WECC		Item 31.2 looks like it should be two separate items. Consider making a separate item for "Test any information used..." at the same required level for high impact.
51.5	City Utilities of Springfield, Missouri	Agree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
51.6	Florida Municipal Power Agency	Agree	30.5 mentions restoring to the previous baseline configuration, without regard to the fact that the baseline may have been the source of the problem. FMPA suggests "prior", giving the RE the flexibility to restore systems based on what they know to be a working system.

#	Organization	Yes or No	Question 51 Comment
51.7	Independent Electricity System Operator	Agree	- R30.1 Please define Recovery Plan. Some regions are not accepting a backup control center, with redundant systems and data as suffice for recovery and think it means building a component from scratch (ie install os, configuration, install application,
51.8	PacifiCorp	Agree	30.4 - Define “protection of information required to successfully restore”.30.5 - The requirement to reinstall and configure any application and system software using its baseline configuration does not consider strategies, such as redundancy or high availability, making the reinstall of a system unlikely and impractical.Define “secure backups” and “functionality”.31.2 - By including the testing of information used in the recovery of BES Cyber systems that is stored on backup media in 31.2 means that Low and Medium Impact BES Cyber Systems do not require testing of such information? If so, it should be a standalone requirement.Define “initially stored”, “useable and current”. This could be interpreted as a full restore to a system, one file being restored as verification that data is not corrupt and process to restore are in place to looking at a tape log and seeing that a backup was made of the data.32.4 and 32.6 - When does the clock start ticking. There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is introduced or is modified. Modifications to the recovery strategy or recovery activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the recovery.31.5 - Does the requirement to update each recovery plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?
51.9	Southern California Edison Company	Agree	The standard should clarify that the time line for the operational exercise that is required by R31.3 is not 36 months for every device is scope, but rather than every disaster recovery plan has to be tested on a scheduled basis.The operational impact of protecting backups at par with operational BES systems is substantial. The backup

#	Organization	Yes or No	Question 51 Comment
			does not support real time BES reliability and should be treated as an ancillary system (i.e. climate control, fire prevention etc.) or similar to systems such as access points and boundary protection devices.
51.10	Alberta Electric System Operator	Disagree	In Table R30, for 30.5, consider changing “known secure backups” to “known good backups” since availability and integrity are more important than confidentiality during system recovery.
51.11	Ameren	Disagree	R30.1 - If you miss listing all conditions or you fail to activate your plan if the certain condition is met makes this difficult to provide complete documentation for an audit. Suggest removal or changing the phrase to "List possible conditions that may activate the recovery plan, update these conditions within 30 days of an actual incident that was not included within the scope of the originally documented conditions."
51.12	American Electric Power	Disagree	31.2: Regarding "Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current", should this be a separate line item? It seems out of place in 31.2.
51.13	APPA Task Force	Disagree	The APPA Task Force supports the drafting team’s efforts on System Recovery. We propose the following edits:31.2, recommend changing “once every 12 months” to “Annually.”32.1, recommend changing “once every 12 months” to “Annually.”32.4, recommend changing “once every 12 months” to “Annually.”
51.14	BGE	Disagree	Provide definition of “operational exercise”
51.15	Bonneville Power Administration	Disagree	The objectives of these requirements (“so that BES Cyber Systems can be restored to a defined state,” “to verify recovery plan readiness and effectiveness,” and “to ensure that the recovery plan(s) will function as intended and that personnel are aware of any relevant changes”) should be clearly labeled as “Objective of Requirement” and shown as a separate sentence prior to the text of the requirement rather than

#	Organization	Yes or No	Question 51 Comment
			appearing at the end of the requirement (i.e., the text of the requirement should not include the objective). That would clearly separate the objective from the action that the Responsible Entity must take.Table R30, Section 30.5 is too prescriptive. For example, one way to do backups is to take a complete image of the system. Restoration becomes merely an issue of restoring that image. There is no need to reinstall and reconfigure. Recommendation: Remove 30.5Table R31, Sections 31.1 and 31.2. There are other ways to test, as well. Testing methods should be devised by the RE, not the standard. The frequency may vary based on the Impact status of the system. However, standardization on the middle ground of at least once every 24 months would simplify compliance.
51.16	Con Edison of New York	Disagree	This criterion should be for control centers or SCADA system only. Many cyber systems which would need to comply with CIP-011 do not have back-ups. The BES can be operated effectively even if other cyber systems are down.
51.17	Constellation Energy Control and Dispatch, LLC	Disagree	Provide a definition of operational exercise.
51.18	Constellation Power Source Generation	Disagree	R31.3 uses the term “representative environment.” At the CIP V4 Workshop, the team stated they used this vague term to give entities flexibility in their operational exercises, but this is not auditable.
51.19	Consultant	Disagree	Table R30 Item 30.5 - First bullet - Suggest changing the word "defined" to "documented" or "identified" or "identified and documented". R23 does not define the baseline.Item 30.5 - Second Bullet - Suggest deleting the words "any" & "most" & "known" & "secure" New wording: "Load information from recent backups." Suggest deleting this bullet. Reloading backup date should be an operational decision made based on the conditions that exist at the time of recovery, and not "forced" by a requirement.Table R32 - Item 31.2 This is two requirements. Suggest separating each into it's own line item.Table R32 - The periodicity requirements of this table should be adjusted. The testing and operational exercise statements are not consistent with the

#	Organization	Yes or No	Question 51 Comment
			incident response plan requirements. Suggest making the requirements for incident response plans and recovery plans consistent.Item 32.2 & 32.3 Suggest changing the word "execution" to "occurrence".Item 32.5 - Actions necessary to address documented plan deficiencies may not be completed within 30 days, so requiring an update to the plan with 30 days would appear to create a situation where compliance is not viable, or sensible. Suggest modifying to be based on completion of corrective actions.Item 32.7 Suggest deleting the word "all" as an unnecessary word.
51.20	CWLP Electric Transmission, Distribution and Operations Department	Disagree	R31.2 the term “current” is not valid if any data has changed since the backup. A backup completed 12 months earlier could never be considered current on an operational system. Consider removing this term.
51.21	Detroit Edison	Disagree	Table 31.2 and 32.1 refer to a period of "12 months". We prefer “at least once per calendar year, not to exceed 14 months between instances”.Table 32.4 should not be an annual update but should be triggered on the required review in 32.2. Consider revising to a sixty day window after the review.Table 32.6 The term "any" is too broad. Consider revising to read "...changes that impact the recovery plan."Table 32.7 Revise "recover" to "recovery"
51.22	Dominion Resources Services, Inc.	Disagree	30.2. The phrase “including identification of the personnel responsible” should be removed from this requirement. Roles and responsibilities should be adequate for the plan. There should not be a need to list 20 relay technicians that could be allowed to recover a substation system. 31.2. The second paragraph of this requirement should be revised to state “Verify BES system can be restored from backup initially and at least annually thereafter”.32.1. The phrase “or when BES Cyber Systems are replaced” should be changed to “or when impacted by BES Cyber System changes.”32.6. The phrase “technology changes” should be changed to “technology changes that impact the recovery plan.” (e.g., not all organizational changes affect the recovery plan.)32.7. The word “recover” should be changed to “recovery”.

#	Organization	Yes or No	Question 51 Comment
51.23	Duke Energy	Disagree	Table 30:30.2 remove “including identification of the personnel”30.3 change ‘personnel responsible’ to “responders”30.5 CIP should not prescribe HOW we restore the system. Suggest removing and adding ‘restoration’ to the list in 30.4Table 31:31.1 multiple plans may be required. Same comment as 28.1 above. Is this once per 12 months per the plan or once per 12 months for each BES cyber system? Suggest allowing 12 months per plan to test.31.2 specify that verifying backup media functionality is an acceptable test.31.3 operational exercises at some generation stations may be unrealistic (unrealistic for availability or costs)Table 32:32.6 this should be part of change managementSuggest allowing 12 months per plan for review.Remove ‘incident’ from 32.2 and 32.3
51.24	EEI	Disagree	Suggested revision for R30.2:Roles and responsibilities of responders, including identification of the personnel (using Job title or job function) responsible for recovery efforts.
51.25	Emerson Process Management	Disagree	It seems there is a conflict between 31.2 and 31.3. If the operational exercise needs to be donw every 36 months per 31.3, then, it should not be needed again every 12 months per 31.2.
51.26	Entergy	Disagree	Entergy agrees for High and Medium Impact Cyber Systems it is important to be able to recover and demonstrate that the recovery plan and backup media used in the process is sufficient to recover the BES Cyber System however, requirement 31.2 and 31.3 appear to be a little redundant although not completely. In requirement 31.3 the entity is required to demonstrate recovery in a representative environment where 31.2 only the backup media is required to be verified as useable and current. Both of these activities provide validation that data can be recovered from the backup media. Requirement 31.3 should be deleted - testing the plan every 12 months either via paper drill or full operational exercise or actual incident coupled with validating the backup media is readable is sufficient to the demonstrate recovery. Requirement 31.1 should be change to include: “Testing any information used in the recovery of

#	Organization	Yes or No	Question 51 Comment
			the BES systems that is stored on backup media when initially stored and at least every 24 months to ensure that the information is useable and current."
51.27	ERCOT ISO	Disagree	30: Request that the use of redundant sites is an acceptable means to address recovery.30.2: Recommend noting what information is necessary here. Are group notifications considered sufficient (e.g., on-call rotations)? 32.2: Should be 30 days rather than 60 days to align with FERC Order 706.
51.28	FirstEnergy Corporation	Disagree	R31 - 31.3 - Need clarity on what is meant by 'Operational' exercise. We believe the intent was business operations, not IT system operations and related DR plan recovery. A business operational exercise is a business continuity planning issue. (example: EMS Operation hot-site testing) Sub-requirement 31.3 would need to be answered by each business unit and not within an IT DR Team response as business operational (BCP) tests are not performed for DR Plans. DR Plans have physical and media type testing which it appears to be what the intent was for 31.1 and 31.2. Need clarity on ownership. It seems like 31.1 and 31.2 are owned by IT, and 31.3 is owned by business units. R32 - 32.6 - We do not agree with changing names in individual recovery plans except during the annual review. Normally organization changes affect the recovery plan approvers list and if changed, would require re-approval of the DR plan. Given the complexity of our critical DR plans, this requirement is not reasonable, and certainly not within a 30 day window - especially if the new name is for someone just starting in a position. We agree that interim organizational changes could be made for call trees of 'personnel expected to respond to/perform a recovery using the recovery plans', but call trees are not part of the individual recovery plans and are instead part of an overall recovery plan. R32 - 32.7 - Recovery is misspelled ('communicate all recover plan...')
51.29	Garland Power and Light	Disagree	Requirement R30 requires the implementation of the plan to be in compliance - Concern is that for some business reason (perhaps a certain business strategy or the economy) some system or facility might not need to be rebuilt. There should be a provision for the Responsible Entity to provide justification to Regional Entity for not

#	Organization	Yes or No	Question 51 Comment
			rebuilding and not be in violation for not implementing and actually rebuilding the "whatever" that failed.
51.30	GE Energy	Disagree	36 months is too long between operational recovery exercises. This should be at maximum 24 months, and should require re-validation if a large system configuration change is made, such as hardware changes, version upgrades, or 3rd party software upgrades.
51.31	GTC & GSOC	Disagree	We recommend R32.1 be changed to the following: "Review and update recovery plan(s) at least once every 12 months or when a Cyber Security Incident recovery of BES Cyber System(s) does not effectively proceed according to the documented plan."We recommend the word "incident" be replaced throughout R30 through R32 with the words "Cyber Security Incident"
51.32	Hydro One	Disagree	Recommend changing the bullets for 30.5 to start with "plans for". The first bullet should be "install" not "reinstall." The recovery plan does not need to include non-BES Cyber Systems. The third bullet should test the BES Cyber System Component(s).
51.33	ISO New England Inc	Disagree	31.2 - "Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current. "impossible to test " - is this to test if your backup works and is usable? Realtime data is never restored - clarification on information and is this test your media for usability? "Test when initially stored"?? Not feasible. More appropriate Verify backup completed successfully, not verify data that was backed up. Control Centers utilize full functioning backup facilities for recovery from the main center being compromised and or rendered unavailable, so for control centers the recovery should be to run from the backup control center once a year. The media should be tested on an annual base to make sure that the data from the offline storage is still recoverable. For facilities that do not have a backup BES cyber systems then I would agree that they need to recover in the way stated. Recommend changing 30.5 bullets to start with "plans for". The first bullet should be "install" not

#	Organization	Yes or No	Question 51 Comment
			"reinstall." Recommend that the recovery plan does not need to include non-BES Cyber Systems. Recommend that the third bullet should test the BES Cyber System Component(s).
51.34	LADWP	Disagree	CIP-011-1 R30 Cyber System Recovery (CSR) should not require to document identification of the personnel responsible for recovery effort (R30.2) within the CSR. Identification of specific personnel will lead to revision of the document when personnel are reassigned.
51.35	Manitoba Hydro	Disagree	The wording of Requirement R31.1 should be revised as the phrase "with a paper drill" could be misinterpreted. There are no specifics given with respect to the Requirements of R30 (in terms of "conditions", "roles and responsibilities", etc., so it assumed to be at the Responsible Entity's discretion in terms of criteria, etc. Consider whether Requirement R31.2 should be two separate Requirements - R31.2 with respect to "Conduct a test..." and R31.3 with respect to "Test any information...". There are no specifics given with respect to "demonstrates readiness" in Requirement R31.3 so it assumed to be at the Responsible Entity's discretion as to whether the test has demonstrated readiness or not. The word "recover" in Requirement R32.7 should be "recovery".
51.36	MidAmerican Energy Company	Disagree	Define "protection of information required to successfully restore".30.5 - The requirement to reinstall and configure any application and system software using its baseline configuration does not consider strategies, such as redundancy or high availability, making the reinstall of a system unlikely and impractical.Define "secure backups" and "functionality".Define "initially stored", "useable and current". This could be interpreted as a full restore to a system, one file being restored as verification that data is not corrupt and process to restore are in place to looking at a tape log and seeing that a backup was made of the data.32.4 and 32.6 - When does the clock start ticking? There could be a series of changes, whether technological or organizational, which is part of a project. What is considered an organizational change? Is it when a phone number changes, a person leaves or when a new role is

#	Organization	Yes or No	Question 51 Comment
			introduced or is modified. Modifications to the recovery strategy or recovery activities should cause an update to the plan, not changes to systems, technology or organization. Changes to those resources may or may not affect the recovery.31.5 - Does the requirement to update each recovery plan based on any documented deficiencies assume that the deficiencies can be resolved prior to the end of thirty calendar days or does the plan get updated with the statement that there is a deficiency?
51.37	Minnesota Power	Disagree	Minnesota Power generally agrees with the proposed Requirements R30, but recommends that the Standards Drafting Team consider defining the term "known secure backups" as it is not currently defined in the Standard and is open to interpretation. Part 31.2 requires that data be "tested" at the time of backup and every 12 months to ensure that it is "useable and current" and to ensure consistency with that requirement, Minnesota Power recommends that the Standards Drafting Team replace "known secure" with "useable". Minnesota Power generally agrees with the proposed Requirements R31, but recommends that the Standards Drafting Team further define what is meant by "test" data stored on backup media to "ensure that the information is useable and current" in Part 31.2. While testing usability can be done by verifying one can read the tapes' contents, how does one test that data is current? This would require more of a manual verification or comparison function than a test, correct? In addition, is R31.3 requiring a full restoration, or is it requiring that each scenario documented in the Restoration Plan be fully tested every 36 months? Minnesota Power recommends that the Standards Drafting Team revise the wording of Part 31.3 to eliminate confusion regarding their intent.Minnesota Power generally agrees with the proposed Requirements R32, but to be consistent with the "update" portion R32, Minnesota Power recommends that Part 32.1 be modified to state "Review the recovery plan(s) at least once every 12 months, or when BES Cyber System(s) have any system, organization or technological changes. Document any identified deficiencies, changes or improvements."Minnesota Power generally agrees with the proposed Requirements R32, but recommends that the term "recover" be

#	Organization	Yes or No	Question 51 Comment
			changed to “recovery” for Part 32.7.
51.38	National Grid	Disagree	National Grid recommends changing 30.5 bullets to start with “plans for”. The first bullet should be “install” not “reinstall.” Also recommends that the recovery plan does not need to include non-BES Cyber Systems and that the third bullet should test the BES Cyber System Component(s).
51.39	Network & Security Technologies Inc	Disagree	30.5 - Suggest revising to require use of either baseline configuration or most recent known “good” configuration. Covers the possibility a (new) baseline configuration is causing problems (can and does happen - even if tests pass).30.5 - Need to define what “secure” backup means.31.2 - Requirement to test information “when initially stored” may be extremely burdensome in some environments, depending on backup mechanisms used. Some types of backup systems use on-the-fly techniques to verify a copy/write operation is “good” but SDT should use language that is less prescriptive. Should also drop the word, “current.” Certain types of operational data will cease to be “current” moments after it is copied. Only real-time mirroring can satisfy this requirement and entities should not be compelled to implement it.
51.40	NextEra Energy Corporate Compliance	Disagree	NextEra believes the CIP-011-1 Table R30 - Recovery Plan Specifications so that BES Cyber Systems can be restored to a defined state did not provide enough guidance and left room for interpretations.The following are the recommended updates:30.1 - The Responsible Entity shall define conditions for activation of the recovery plan(s).30.4 - Processes and procedures for the backup, storage and protection of information required to successfully restore a BES Cyber System30.5 - Implement a test plan to identify the processes and procedures for the restoration of BES Cyber Systems to include the following: o Reinstall and configure any application and system software using its baseline configuration defined in Requirement R23, o Load any information from the most recent, known secure backups, o Conduct a system test to verify functionalityModified the wording and additional guidance should be provided by NERC on the minimum conditions which would activate the plan.NextEra also believes that Table R31 - Recovery Plan Testing Specifications to verify recovery

#	Organization	Yes or No	Question 51 Comment
			plan readiness and effectiveness did not talk about documenting test resultsThere should be documentation of test results to validate that it was performed. The following are the recommended updates:31.1 - Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 24 months. All testing results shall be documented.31.2 - Conduct a test (by recovering from an actual incident, with a paper drill, or with a full operational exercise) of the recovery plan at least once every 12 months. Test any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored and at least every 12 months to ensure that the information is useable and current. All testing results shall be documented.31.3 - Conduct an operational exercise at least once every thirty-six months that demonstrates recovery in a representative environment unless an actual incident response occurred within the thirty-six month timeframe that demonstrates readiness. All testing results shall be documented.In 30.5, the recovery plan expands the current backup and restore of any application and system software using its baseline configuration. Is the definition of baseline the current or previous version of an application and system software?In 31.2, does the testing of any information used in the recovery of BES Cyber systems that is stored on backup media when initially stored to ensure that the information is useable and current require the Responsible Entity to "load back" the data that is stored on backup media to an operational system to prove usability? Is loading it back to a test environment sufficient?In 31.2, "Test any information used in the recovery of BES Cyber systems." Does the requirement imply that in the case of protective relays at a BES Transmission Facilities, the backup settings file for every protective relay at High Impact facilities should be tested every 12 months?
51.41	Northeast Power Coordinating Council	Disagree	Recommend changing the bullets for 30.5 to start with “plans for”. The first bullet should be “install” not “reinstall.” The recovery plan does not need to include non-BES Cyber Systems. The third bullet should test the BES Cyber System Component(s).
51.42	Oncor Electric Delivery LLC	Disagree	These requirements are unnecessarily burdensome. Entities have been recovering from man-made and natural disasters for many years without these requirements.

#	Organization	Yes or No	Question 51 Comment
			Entities should be able to leverage Business Continuity, High Availability architectures and Standardization to demonstrate their ability to recover from unforeseen events. Requirement 32.6, update of Recovery Plan, we suggest this review be conducted quarterly.
51.43	Progress Energy - Nuclear Generation	Disagree	Agree with R30 and R31. Disagree with R32. Incorporating information contained in the matrix in Attachment 1 which aligns CIP 011-1 Requirements with CFR(s), National Institute of Science and Technology (NIST) and Nuclear Regulatory Commission accepted NEI 08-09 Rev. 6 Nuclear Cyber Security Plans for comments for consistency in regulation for R30-32.
51.44	Progress Energy (non-Nuclear)	Disagree	R30.5 the first bullet should not be a requirement based on the second bullet.
51.45	Regulatory Compliance	Disagree	30.5 - STTRKE all the bullet points. Recovery plan should be system wide. Test restoration annually - document processes.31.2 - Make the second item a separate criteria line item - it's too confusing the way it is currently written. "Required" for High Impact.32.2 - "Annually" review the results.....
51.46	ReliabilityFirst Staff	Disagree	For R30, change “or failure” to “failure, or destruction.” For 30.4, please clarify what is meant by “successfully restore”. For R30.5, please clarify what is meant by “known secure backups”. For R31.3, change “incident response” to “activation of the recovery plan”. For R32, delete “relevant” so all changes are communicated. For R32.7, change “recover” to “recovery”.
51.47	ReymannGroup, Inc.	Disagree	R30.4 should be expanded to include processes for the recovery, restoration, and protection of data from a damaged or failed BES Cyber System. R30.5 should be expanded to include a review to ensure that malicious code has not been installed on the recovered files or device.
51.48	RRI Energy	Disagree	What constitutes a representative environment?

#	Organization	Yes or No	Question 51 Comment
51.49	San Diego Gas and Electric Co.	Disagree	R30 - R32 were originally covered in CIP-009-3. Referencing Table R30 - SDG&E suggests that R30.4 and R30.5 be removed. The IT Disaster Recovery Plan covers this and it would not normally be part of our Business Continuity Recovery Plan. The Responsible Entity (RE) should not be required to develop Recovery Plans with detailed IT processes for storage, backup, protection and reinstallation of software, etc. Referencing Table R31 criteria 31.3, SDG&E suggests that this wording be changed. CIP-009-3 R2 provides the RE with more options for "exercising" the recovery plan and we prefer the way the Requirement is worded in CIP-009. Referencing Table R32, CIP-009-3 R3 provides the RE more options when developing plans and procedures to comply with the Requirements. The new table seems to hold the Entities (both Medium and High) to several compliance timetables that are extremely restrictive. SDG&E suggests that we utilize the same wording for this Requirement from CIP-009-3 R3.
51.50	Southwest Power Pool Regional Entity	Disagree	R30: Is a recovery plan required for each BS Cyber System or is a generic plan acceptable? Recovery plans need to range from device component failure to catastrophic failure (e.g. physical facility disaster). 30.2: Is the identification by individual name or by position title? 30.5: What is meant by "secure" backups? Encrypted? Securely stored? Something else? Also, the backup and restoration processes should be "as applicable." Not all recovered systems are restored from a "backup." 31.2: Does the requirement to test backup media when initially stored apply to every daily backup, or only after BES Cyber System updates? Does the test include a restoration to an offline environment to verify the backup is not only readable but also complete? 31.3: Clarify that the operational exercise is more than a system or site fail over (NERC Standard EOP-008 exercise) but must also include performing the necessary steps to recover from the failure and restore the failed systems to normal operation by following the steps of the plan. 32.1: Include BES Cyber Systems that are significantly updated / upgraded requiring an update to the recovery plan. 32.4: Require the update within a much shorter time following determination of the need through the methods defined in the criteria. Delayed

#	Organization	Yes or No	Question 51 Comment
			updates are at risk of being overlooked and out of date plans pose a risk to the entity's ability to quickly recover. 60 days is recommended.
51.51	USACE - Omaha Anchor	Disagree	A) 30.5 - how often must system test be conducted? B) 31.2 Clarify "initially stored" is this the first time the tape is used?C) 32.6 - this could be interpreted to require a change in the recovery plan every time a software change occurs. This is very extensive - and unrealistic. Potential verbiage could be 'whenever system, organizational, or technology changes effect the recovery plan.'
51.52	We Energies	Disagree	We Energies agrees with EEI: Suggested revision for R30.2:Roles and responsibilities of responders, including identification of the personnel (using Job title or job function) responsible for recovery efforts.
51.53	Xcel Energy	Disagree	Definition is needed as to what constitutes an "operational Exercise". Is this a table top drill, or something more.

52. Tables R30 to R32 provide direction concerning what impact level of BES Cyber Systems to which Requirements R30 to R32 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Summary Consideration:

Note that "Recovery Plans" are now addressed in CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems

The primary focus areas of the comments were concerned improving the clarity of the periodic timing requirements and the large amount of test equipment it would take to develop representative environments for numerous disparate facilities.

Some commenters noted the different terms used for references to annual activities. The SDT reviewed the use of annual, calendar year, 12 months, etc. and in the revised standards used the phrase, ". . .at least once each calendar year, not to exceed 15 calendar months between. . ."

There were suggestions that the testing requirements should only apply to control centers as Recovery Plans apply to Medium & High Impact Level categorizations, while some aspects of the recovery plan may only apply to High Impact assets. Additional guidance was requested for operational testing and for testing of information that is stored on backup media. The SDT added some information about testing in the Rationale Box for Requirement R1 in the revised CIP-009-5. Testing is necessary to verify the Responsible Entities Recovery Plan's effectiveness. Planned and unplanned maintenance activities may also present opportunities to execute and document an Operational Exercise (see NIST SP 800-84, Functional Exercise). This is often applicable to operational systems where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

Issues identified in comments for SDT consideration were Recovery Testing – Operational Test every 36 months should count for the annual test, recovery plan testing clarifications, data retention plan clarification, identification requirements of "Personnel Responsible", coordination of physical aspects of Cyber Security Incidents, and incident recovery plan reviews. The SDT notes that there are FERC directives (e.g., P686, P687, P725) to add a requirement to conduct a full operational test of the recovery plan once every three years – so the suggestion to count the full operational test as the annual test was not adopted. (CIP-009-5 R2)

Commenters suggested changes and provided various requests/suggestions for re-wording/wordsmithing and improved coordination of backup and recovery with EOP-008. The SDT has coordinated its proposed requirements with the now FERC approved EOP-008-1 – Loss of Control Center Functionality. Commenters suggested that all requirements should be in the table, not in the objective or in the "pre-amble" to the requirements and that the SDT consider providing a summary table for all periodic requirements and remove the "how to" statements from the requirements. The SDT has included all mandatory performance in the requirements of the revised standards. The SDT did not adopt the suggestion to develop a summary table for periodic requirements as the format for Version 5 is considerably different from the format proposed when the requirements were all combined in CIP-011.

	Organization	Yes or No	Question 52 Comment
52.1	Alberta Electric System Operator	Agree	There appears to be a typo in 32.7 - "Communicate all recover plan updates" - recover should be recovery.
52.2	Emerson Process Management	Agree	In reality, it would be a good practice to exercise recovery plan during or toward the end of each scheduled unit outage for generation.
52.3	Florida Municipal Power Agency	Agree	FMPA suggests changing “12 months” to “annual” and “24 months” to “biennial”
52.4	PacifiCorp	Agree	31.2 - By including the testing of information used in the recovery of BES Cyber systems that is stored on backup media in 31.2 means that Low and Medium Impact BES Cyber Systems do not require testing of such information? If so, it should be a standalone requirement.
52.5	American Municipal Power	Disagree	Please provide a little or no impact category
52.6	American Transmission Company	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.7	APPA Task Force	Disagree	The APPA Task Force supports the MRO-NSRS comments on impact levels and therefore proposes the following changes:R31 Table 31.3: Low Impact: N/AMedium Impact: N/AHigh Impact: Required for Control Centers OnlyThe APPA Task Force agrees with the impact levels for the rest of R30-R32 if it is understood that a blank in the table means N/A.
52.8	BGE	Disagree	R30 - R32 should synchronized with R29 to include both Low and medium impacted

	Organization	Yes or No	Question 52 Comment
			BES Cyber Systems.
52.9	Black Hills Corporation	Disagree	30.4 should also apply to Medium Impact systems. Without this basic information, recovery would have to start from scratch.
52.10	Bonneville Power Administration	Disagree	Table R32Sections 32.2 and 32.3. Both should allow 60 days for review.Section 32.4: 12 months is too long. No more than 6 months should be allowed. Items 31.1 through 31.3 in Table R31 and 32.1 and 32.4 in Table R32 states certain events must occur "at least once every 12, 24, or 36 months." Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. The SDT should be very specific as to what it means for how frequently the events referenced above must occur.
52.11	City Utilities of Springfield, Missouri	Disagree	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
52.12	Con Edison of New York	Disagree	See 51
52.13	Consultant	Disagree	Table R30 - It doesn't appear to make sense that the Recovery Plans applies to Medium & High impact level categorizations, while aspects of the recovery plan only applies to High Impact assets.Table R31 & R32 - How many test and exercises are required? The structure here will create an administrative burden to track what was done when that has no corresponding risk reduction.Mixed requirements would force multiple recovery plans based on categorization of assets, which could mean two recovery plans for the same asset type where the application of each asset has a different impact categorization. This does not appear to be a sensible approach to recovery plans.Suggest deciding on a consistent set of requirements that can be applied equally to High Impact and Medium Impact assets.
52.14	CWLP Electric Transmission, Distribution	Disagree	R32.6. In order to meet the required change management process in R23 this window should be extended to 60 days.

	Organization	Yes or No	Question 52 Comment
	and Operations Department		
52.15	ERCOT ISO	Disagree	All requirements should apply to Medium Impact BES Cyber System due to interconnectivity to other BES Cyber Systems.
52.16	FirstEnergy Corporation	Disagree	R32 - Combine R32.5 and R32.6 and eliminate the word 'organizational'.
52.17	Garland Power and Light	Disagree	Requirements 30.1 & 30.2 - remove Medium Impact classification
52.18	ISO New England Inc	Disagree	32.6 - clarification on scope of "any" technology and system change scope. (organizational change is fine). R32.7 spelling "recover" should be recovery? CIP Standard use of the term "annual": The term "annual" should be replaced with the phrase: "no fewer than X (e.g. 9) months, but no greater than Y (e.g. 18) months". The time duration in "X" and "Y" should be clarified by the Standard Drafting Team, taking into consideration the appropriate level of exposure the time duration would provide. This phrase would provide Registered Entities with flexibility within any given calendar year to accomplish the prescribed action, but at the same time restrict companies from taking action in December of one calendar year, and then again in January of the next.
52.19	LADWP	Disagree	Medium Impact should not be a factor.
52.20	Lincoln Electric System	Disagree	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
52.21	Manitoba Hydro	Disagree	Medium Impact BES Cyber System should be included as "Required" in sections 30.3 to 30.5
52.22	MidAmerican Energy Company	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous

	Organization	Yes or No	Question 52 Comment
			disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.23	MRO's NERC Standards Review Subcommittee	Disagree	Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.24	Oncor Electric Delivery LLC	Disagree	Verification of the entity's Recovery Plan for High Cyber Systems every 12 months should cover Requirement 31.1. This should require only one test for the entity - remove low/medium/high)
52.25	Progress Energy (non-Nuclear)	Disagree	See comment 14.What is meant by an operational exercise in a representative environment? Does it mean individual components that can be easily tested for recovery plans?
52.26	ReliabilityFirst Staff	Disagree	For R30, each subrequirement should be "Required" for all the "Medium" impact BES Cyber Systems. For R32.6, should be "Required" for "Medium".
52.27	San Diego Gas and Electric Co.	Disagree	SDG&E would agree with Table R30 if item 30.5 were to be removed. Similarly, SDG&E would agree with Table R31 if item 31.3 were to be removed. Referencing Table R32 - SDG&E prefers the wording in CIP-009 R3 in this area because it provides more flexibility for the Entities while still covering the issues.
52.28	Southern California Edison Company	Disagree	The drafting team should state in CIP 010 that back-up systems should be treated at par with system key to real time BES reliability if the intent of this requirement is that CIP-011 be applied to all BES systems.
52.29	Southwest Power Pool	Disagree	30.3, 30.4, and 30.5 should be applicable to Medium impact systems. 32.6 should be

	Organization	Yes or No	Question 52 Comment
	Regional Entity		applicable to Medium impact systems with perhaps a 60-day update timeframe.
52.30	The Empire District Electric Company	Disagree	Comments: Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.
52.31	WECC	Disagree	All items should be required for medium impact levels in R30Criteria should apply to all impact levels.

53. Which requirements in draft CIP-011-1 should allow for TFE submissions? Note that not all requirements will be considered as being applicable for TFE submissions. The drafting team has attempted to minimize the need for TFEs by modifying the language to allow for flexibility in meeting the requirements. Please provide suggestions on how the language of the standard may be modified to eliminate the need for TFEs. If TFEs are still needed, please provide specific examples to justify the inclusion of a requirement as being TFE eligible.

Summary Consideration:

Some commenters stated that the requirements should be written around the specific device types. The drafting team considered this option, but believes that it becomes problematic for entities and auditors to determine when a device is multi-purpose versus purpose-built. Some purpose-built devices can be considered multi-purpose depending on how the device was manufactured and implemented.

A variety of comments were received regarding the TFE process and its applicability to the specific CIP Cyber Security requirements. While the TFE process itself was outside the scope of the drafting team's work, commenters stated that TFEs should be allowed for passwords, malicious code monitoring, system hardening, system event monitoring, wireless and remote access, as well as for communications and data integrity. The drafting team considered these comments and revised the requirement text where necessary to allow entities more flexibility in implementing these requirements thereby reducing the need for TFEs. In some cases, the requirement was removed or written at a system level to prevent the need for TFEs.

#	Organization	Question 53 Comment
53.1	Detroit Edison	14.4, 17.1, 17.2, 16.2, 10.1-10.8 should retain TFE status.
53.2	Network & Security Technologies Inc	19.1 (see comments on Question 35), 26.2 (see comments on Question 47)
53.3	ISO New England Inc	Actual language on several requirements need to be clarified, many are still open to interpretation which may lead to TFE's.
53.4	EEI	Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.

#	Organization	Question 53 Comment
53.5	Progress Energy - Nuclear Generation	All CIP 011-1 Requirements should contain provisions similar to NIST 800-53, Regulatory Guide (RG) 5.71, and NEI 08-09, Revision 6, CIP standards should provide for nuclear facilities' use of alternative methods which implement security controls equivalent to those required by CIP. Nuclear programs, required by regulation, currently in place at nuclear facilities provide these alternate methods. Technical Feasibility Evaluations (TFE) should not be required with such documentation. One example is that nuclear facilities have one of the most effective Physical Security Programs of Critical Infrastructures. CIP-011-1 requirements R5 and R6 should acknowledge nuclear generating station physical security programs.
53.6	Ameren	All of the following requirements would need a TFE o R10 for passwords complexity o R14.4 for user banners o R15 for malicious code protection o R16 for installing patches o R18 for logging security events o R19 for validating data inbound o R23.7 for monitoring changes to a baseline configuration.
53.7	US Army Corps of Engineers, Omaha Distirc	All requirements that require existing hardware and software be capable of performing any function should allow for the possibility of TFE's. Sections R10, R15, R17, R18, R19, & R23 have requirements that are likely to require TFE's.
53.8	Southwest Power Pool Regional Entity	Any time a requirement specifies "continuous", "all", or prescribes a specific solution or characteristics of a technical solution, a TFE may be necessary. Try to avoid specific technology requirements as discussed elsewhere in these submitted comments.
53.9	The Empire District Electric Company	Comments: See comments under questions 34, 35, and 37.
53.10	RRI Energy	Cyber assets that are not on your standard IT equipment list are the most likely devices to need TFEs. This list could include meters, vibration monitors, PLCs, DCS, RTUs, cpu based test equipment.
53.11	E.ON U.S.	E.ON U.S. believes that many of the requirements remain ambiguous and additional clarity is needed. Absent such clarity it is difficult to ascertain where TFE ability can be eliminated. In fact, the proposal to provide greater compliance flexibility for responsible entities makes this determination even more difficult. As the requirements currently read, E.ON U.S. believes that more, not less, TFE requests will

#	Organization	Question 53 Comment
		result. Areas where responsible entities have requested additional clarity need to be addressed prior to issuance of a final industry draft. The informal comment period does not provide an adequate forum to identify all areas of concern and suggest specific replacement language.
53.12	Cogeneration Association of California and Energy Producers & Users Coalition	Entities should be able to use TFEs for any instance where unsupported technology is in place that may not be compliant with CIP-011 requirements due to age or vendor proprietary technology. Patches, updates, virus scanning, or firewalls may not be available for older, unsupported technology. An entity should not be required to upgrade or replace a system that currently satisfies the needs of the entity. The entity should be able to use other mitigation methods to protect a system if patches, updates, virus scanning, or firewalls cannot be applied.
53.13	Northeast Utilities	Equipment that never has security software patches or virus protection should be exempt. Also, those cyber assets that do not have user authentication capabilities should be exempt from password requirements.
53.14	ERCOT ISO	ERCOT ISO supports the proposed form of combining all requirements into a single reliability standard. The use of a single standard will eliminate the need for cross-referencing to other reliability standards. ERCOT ISO does request a realignment of some requirements. All requirements for access authorization, revocation, and review should be combined to eliminate confusion of how access should be managed.The timing of updates to documentation should be consistent throughout the requirements. Recommend the use of 30 days to be in compliance with the directives of FERC Order 706.
53.15	Bonneville Power Administration	If the standards present the overall security controls required, and do not attempt to dictate how those controls are accomplished, there should be no need for TFEs.If there is a need:First, the TFE process as presently constituted has shown to be cumbersome, not well understood, and inflexible. Neither NERC nor The Regional Entities have the detailed internal system knowledge or manpower to do make an intelligent judgment. At best, they can make a broad, industry best guess. The TFE approval process belongs within the Responsible Entity, at a technical level where there are people who know the environment, the systems, and their capabilities can evaluate them. They should be audited as part of the normal compliance audit.Second, if a system will not, or can not perform a

#	Organization	Question 53 Comment
		required function, it should be up to the RE to determine what steps should be taken to meet the standard. Third, because there are so many ways to accomplish the security of systems, the only time a TFE should be necessary is when all methods have been exhausted that could provide a level of protection required.That being said - Any time a situation arises where for technical reasons, or because implementation of security features may present BES reliability issues, or where application of one security measure would compromise others, the RE should have the authority to choose how to proceed. If this is called a TFE, the RE should approve it and document it as part of the overall security planEven if TFEs with approval required by the REs or NERC are used under CIP-010 and CIP-011, the process needs to be revised. As examples:1. There needs to be an opportunity for entities to appeal or request reconsideration of a rejection of the initial submission. Under the current, at best they can resubmit one time to correct errors.2. It should be possible to submit TFEs under multiple justifications.3. There are claims that the regional entities have been instructed to reject any TFEs other than those based on legacy equipment. If true, this violates the process, which allows TFEs for both new and legacy systems. It is also unreasonable: there are still systems today, and will be for the foreseeable future, that may be the best overall solution for reliable operation of the grid but which do not allow full compliance. Having said that:10.6 may not be possible for all systems. For overly simplistic example, routers intended for small office/home office use often allow either full access or no access. If all that is necessary is to review a log, full administrative access is overkill. To avoid the need for a TFE, recommend "To the extent possible for the particular device or system, require that authorized..."10.8. Same comment as 10.6.14.2. Unless the definitions of external connectivity and/or remote access or change, 14.2 may not be possible in every instance. For example, consider a legacy multi-user system in a Control Center that is not capable of multi-factor authentication. Any access from a system not part of the BES Cyber System containng the legacy system would constitute remote access and require multi-factor authentication for a High Impact system. It is not clear from R14 whether that multi-factor authentication is required at the BES Cyber System itself or at the access point. If it is required at the system itself, then a TFE would be required. Recommendation: Redefine external connectivity and remote access as described above. Multi-factor could then be required clearly at the external access point.14.4. It is not always possible to display an appropriate use banner under such circumstances. As an example, consider remote connection using a VPN. The access point in that case would the device at the endbound end of the encrypted tunnel. The user never sees a

#	Organization	Question 53 Comment
		screen on that access point, and therefore sees no such banner. Recommendation: See the suggested revisions to 14.4 R19. For both 19.1 and 19.2, validation might not be possible. In particular, commercial off the shelf software (COTS) may or may not provide such validation. If the COTS is the best solution otherwise, a TFE would be required.
53.16	Public Service Enterprise Group companies	Implementation of requirements 10 (Response to Question 24), 13(Response to Question 32), 23.7 (Response to Question 40) and 26.2 (Response to Question 48) may not be feasible in all situations. Please see comments in the questions that relate to these requirements for description of the potential infeasibility.
53.17	Idaho Power Company	In R19, data validation and encryption may in some control center applications, introduce a data latency that renders the application degraded or useless and may result in a more secure environment but less reliability. In R19.2, I am unaware of technology that can determine whether invalid data has been maliciously compromised. Most EMS/SCADA systems which would be the most common BES cyber system in a control center filter or ignore invalid data anyway and I do not see that the benefit of this requirement outweighs the technology investment needed to meet this requirement.The ability to alert on unauthorized access attempts may require a TFE depending on the boundary device that is protecting the system. Some boundary devices do not lend themselves to providing alerting and may require a TFE until they are replaced with a device that can meet this requirement.
53.18	Lincoln Electric System	LES supports the comments submitted by the MRO NERC Standards Review Subcommittee (MRO NSRS).
53.19	MidAmerican Energy Company	MidAmerican Energy agrees with EEI's comment below:Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.
53.20	Minnesota Power	Minnesota Power recommends that the following requirements should still be eligible for Technical Feasibility Exceptions:Requirement 8, Part 8.3:Depending on the definition of “monitor the use,” it may be impossible to do this for many devices. For example, for Windows computers, how does one monitor the use of someone when much of the interaction involves mouse clicks? Will software be

#	Organization	Question 53 Comment
		required to log, not just keystrokes, but mouse clicks? Further, certain devices do not even maintain an audit trail of logins/logouts (e.g.: networked KVMs for remote console access to servers to allow for efficient system administration).Requirement 10, Part 10.2:While this is certainly good IT Security practice, implementing this on every BES Cyber System could very well put the reliability of the BES at greater risk. Since there is no way to change all passwords in all the various devices simultaneously, especially in a utility that is geographically distributed and remote, this will result in a continual need to change passwords. As a result, it could become commonplace for technicians and engineers to not know/remember what password to use on what device. Not only will this keep them from accessing devices at potentially critical times to perform needed maintenance, but EVERY failed login attempt will then have to be investigated in detail. This could be minimized by requiring this for only Medium and High Impact systems.Requirement 10, Parts 10.4 and 10.5:It is quite probable that devices exist that cannot meet these requirements.Requirement 10, Parts 10.8:It is quite probable that devices exist that do not allow for the creation of accounts, whereby all functions must be performed from the system/admin account(s).Requirement 15:For any BES Cyber Systems that are not on routable protocol networks, it is not possible to have network-based malware detection/prevention. Thus, if the device itself does not support the installation of malware-prevention software, Requirement R15 would be not technically feasible.Requirement 18:For any BES Cyber Systems that are not on routable protocol networks, it is not possible to have network-based malware detection/prevention. Thus, if the device itself does not support the security event logging, R18 would be not technically feasible.Requirement 19:The way this is written, the requirement is likely technically infeasible for most any system. To correct, Part 19.1 could be changed by replacing the word “Validate” with “Encrypt”.Requirement 23, Part 23.7:This implies detecting changes that have occurred outside of the approved methods of Parts 23.3-23.6. As such, not all devices may support the installation of software that would allow for such monitoring.
53.21	Progress Energy (non-Nuclear)	Need to include language that allows for procedural controls - example as for password requirements which cannot typically be enforced technologically.
53.22	WECC	No requirements should be so prescriptive to required a TFE. The SDT has done a good job in rewriting requirements to describe WHAT is required without describing HOW it must be achieved.It is impossible to draft standards language that anticipates all possible limitations for implementation.

#	Organization	Question 53 Comment
		The standards, or Rules of Procedure should allow for exceptions to any requirement if an entity could provide justifiable basis and acceptable alternative controls.
53.23	Nuclear Energy Institute	Older computer based equipment may not support all of the controls such as logging/monitoring and accounts/passwords. Alternate controls should be allowed in these cases.
53.24	PacifiCorp	PacifiCorp agrees with EEI's comment below:Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.R10 - equipment still exists in the field that cannot meet the requirement of a 6 character password. R14 - equipment still exists in the field that cannot meet the requirements.
53.25	Dominion Resources Services, Inc.	Please see Dominion's responses above suggesting the addition of footnotes to avoid required TFEs for requirements 10.8, 14.4, 15.2, 15.3, 18.2, 26.2.
53.26	Puget Sound Energy	Puget Sound Energy suggests Table 10, Table 18, and Table 22 as inclusive for TFE eligibility for the following reasons (also stated in those sections):Table 10 - Puget Sound Energy suggests including "Where Technically Feasible" to R10, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 10.Table 18 - Puget Sound Energy suggests including "Where Technically Feasible" to R18, as some BES Cyber Systems may be incapable of meeting all the requirements in Table 18. For example, entities may incorporate dialup accessible devices that, by the nature of a connection that is built up and torn down as necessary, is incapable of providing "continuous security monitoring that issues alerts".Puget Sound Energy suggests including "Where Technically Feasible" to R22, as some Protective Cyber Systems may be incapable of meeting all the requirements in Table 22.
53.27	FEUS	R10: Access Controls; some legacy systems do not allow for default factory accounts to be changed; some legacy systems only allow for a single level of access.R14: For systems not connected to an external network that use Dial-Up access for remote support multifactor authentication may not be technically feasible. Keeping some systems/networks separate from an external cooperate network can reduce cyber vulnerabilities.

#	Organization	Question 53 Comment
53.28	Southern California Edison Company	R7.2: Enforcing this control may be limited by the technical capability of a SCADA device. A device such a PLC that has preset accounts forces the RE to develop acceptable use for a set of accounts retroactively rather than have the capability to limit the account types.R10.4 and R10.5: There are SCADA devices in service that are not at the end of their service life that do not offer this capability. R15.1, 15.2 and 15.3: While these capabilities may be possible at the electronic boundary, individual SCADA devices may not support this functionality. Strict compliance is restricted by technical limitation.R17.1: The mitigation plan that is suggested should be a part of a formal technical feasibility exception program.R28.1: The phrase "or a full operational exercise" is expected to result in technical feasibility exceptions since this will require test data/ setting to be loaded onto in-service SCADA systems.
53.29	Alliant Energy	Recommended changes for any TFE program implemented:Security patch TFEs should be programmatic and not based on individual patch releases.Cyber Asset counts should be stricken. Approved changes to the environment create an immediate ad-hoc obligation for TFE update to the RRO for what is already a burdensome process.Quarterly updates should be removed and replaced by re-approval on an annual basis by the Sr. Manager or delegate.NERC should create a standard Class-Type list as originally proposed.
53.30	USACE HQ	Requirements 10, 14.4, 15 and 17, among others, should have a TFE.
53.31	San Diego Gas and Electric Co.	SDG&E recommends that the TFE processes be changed and incorporated into the Vulnerability Management Process; where the Entity would identify, track, and mitigate any TFEs as a Vulnerability. This methodology will streamline and enhance the TFE process and thereby 1) allow Entities to manage their TFE's internally, 2) reduce Entity, NERC, Reliability Coordinators and Regional Reliability Organization resource requirements, 3) reduce paperwork, resources, and overhead, 4) reduce the potential for errors or leakage of secured information, 5) enhance the audit process and 6) standardize and clarify the process across all Entities.
53.32	BGE	See comments for R13 under Q31-31 and R23 comments under Q40-41.

#	Organization	Question 53 Comment
53.33	MRO's NERC Standards Review Subcommittee	See comments under questions 17, 34, 35, and 37.
53.34	American Transmission Company	See comments under questions 34, 35, and 37.
53.35	Florida Municipal Power Agency	See comments under R7, R14, R16, R23, R20
53.36	CenterPoint Energy	See references to possible TFE issues in comments above.
53.37	SCE&G	Similar to RG 5.71 and NEI 08-09, allowances should be provided for use of alternatives to the required security controls. Alternate controls would be justified and documented that the Threat Vector has been mitigated. TFEs are administartively burdomesome and currently require annual certification and ultimate elimination. The scope of equipment eligible for TFEs will drastically increase the number of filed TFEs, especially for eligble requirements with low impact categories. The SDT needs to consider the feasibility and practicality of implementing the current TFE process with these standards.
53.38	ReliabilityFirst Staff	Table R10, requirements 10.1 and 10.2, Table R14, requirement 14.4, requirement R15, Table R19, requirement 19.2.
53.39	Consultant	Technical Feasibility Exceptions should be allow for any requirement. There are about 2,000 registered entities. Trying to address every configuration of every asset across that spectrum would result in either the requirements being written in a convoluted and confusing manner to address the multiple configurations or being written with little detail to allow the multiple configurations, neither of which could even approach a "bright lines" concept of the requirements. The Technical Feasibility Exception should include a technical basis that shows implementing the specific requirement as stated would not achieve the requirement objective, or improve the security position as it relates to the requirement objective.The Technical Feasibility Exception process probably needs to be improved to deal with exceptions as described here.

#	Organization	Question 53 Comment
53.40	Kansas City Power & Light	TFE should continue to be allowed. Unsure of all the requirements that this may apply to at this point. Recommend the Drafting Team at least consider a direct translation from the CIP version 2 requirements to these CIP-011 requirements at a minimum since CIP-011 is intended to be a translation but less prescriptive.
53.41	USACE - Omaha Anchor	TFE's will still be required in several standards - I've addressed the requirement for TFE in applicable standards.
53.42	Allegheny Energy Supply	TFEs can be reduced by providing additional language in the standard that recognizes the limitations of certain BES Cyber Components.
53.43	Allegheny Power	TFEs can be reduced by providing additional language in the standard that recognizes the limitations of certain BES Cyber Components.
53.44	National Grid	TFEs related to Password and Appropriate Use Banner.
53.45	CWLP Electric Transmission, Distribution and Operations Department	TFEs should be allowed for requirements R10, R13, R14, R15, R16, R17, R18, R19, and R23.
53.46	Reliability & Compliance Group	The best thing that could be done for this Standard is to ensure that everything is well defined so that there is no ambiguity when it comes to identifying BES Cyber Systems and also categorizing their impact.
53.47	Manitoba Hydro	The language or the requirements should be written such that there should be no need for TFE submissions. The standards should allow for compensating measures. For all instances where it is not technically possible to meet strict compliance with a requirement, the Responsible Entity should apply compensating controls which are documented and approved by the senior manager or delegate, similar to the policy exception process in CIP-003-1. The current TFE process creates a enormous administrative burden on the electric industry which provides no additional value to the reliability of

#	Organization	Question 53 Comment
		the Bulk Electric System.
53.48	LADWP	The need for TFEs still exist as certain control systems are legacy systems that may not have current update or patch capability (e.g. SCADA systems). Removal of TFEs for these systems would result in non-compliance as replacement or upgrade of these systems must be done on a planned and scheduled manner.
53.49	Garland Power and Light	There are 2 requirements specifically listed below that need TFE's but there should be provision for any equipment that cannot be made strictly compliant with any requirement that either a TFE or a mitigation plan can be written and implemented such as is stated in 16.1 or 17.1.Requirement R10 - Unless the requirement is rewritten to allow for procedural controls to suffice for compliance or the language in the footnote is actually included in the requirement, a TFE is needed for this requirementRequirement R14 - A printed circuit board (with a network connection) in most cases will not allow for any process to be loaded onto it to protect against malicious software - need a TFE for this requirement
53.50	GE Energy	These changes should eliminate the need for the vast majority of TFEs. There may still be a requirement for TFEs on systems that cannot enforce the password complexity rules.
53.51	FirstEnergy Corporation	This question should be postponed until the Standards are in a more final state so that entities can better see how the new requirements would apply to specific devices, etc. It appears that R20 would necessitate new TFEs.
53.52	NextEra Energy Corporate Compliance	Though NextEra believes TFEs are very important part of the CIP process, given the number of changes proposed, NextEra will wait until the next draft to comment on TFEs.
53.53	Oncor Electric Delivery LLC	To eliminate the need for TFE’s the standard will have to be more granular. Many legacy systems are immune to cyber attacks, yet cannot satisfy the requirements of this standard. R8.3 as an example, there is no system to monitor access at the physical port of relays. R10 - legacy devices do not support account management.

#	Organization	Question 53 Comment
53.54	American Electric Power	We encourage the SDT efforts in drafting requirements in such a manner that will eliminate the need for a TFE. The TFE process should be standardized between the Regional Entities. Currently, Responsible Entities are required to submit multiple forms and varying information for the TFE process depending on the Regional Entity. AEP suggests standardizing on a single submission form and process and have all TFE data submitted to a single source maintained by NERC that can be used by all Regional Entities. This will allow Responsible Entities to submit and/or modify TFE data once and have it available to all Regional Entities on a consistently.See comments under questions 24 and 35.
53.55	We Energies	We Energies agrees with EEI: Additional language regarding the features and functions of devices need to be added to the requirements. TFEs can be reduced by providing additional language that recognizes limitations of certain equipment.
53.56	Regulatory Compliance	We feel that TFE's should still be considered for the following tables:R10 - Account Access Control SpecificationsR14 - Wireless and Remote Access ControlsR16 - Security Patch ManagementR17 - System HardeningR18 - Security Event MonitoringR19 - Communications and Data IntegrityR20 - Electronic Boundary ProtectionR23 - Configuration Change Management
53.57	BCTC	We have embedded this information in our individual responses to previosu questions.
53.58	US Bureau of Reclamation	We have not had an opportunity to assess which requirements may require a TFE yet. We will evaluate the requirements during the next evaluation period.
53.59	Duke Energy	We prefer that all of the requirements allow for an exception. Older computer based equipment may not support all of the controls such as logging/monitoring and accounts/passwords. Alternate controls should be allowed in these cases.
53.60	GTC & GSOC	We recommend that TFEs should be considered for all requirements with the exception R1 because of the ability of the regional entity and NERC to review the appropriateness of the TFE. We recommend adding language to the requirements on acceptable use banners and passwords to clarify that they do not require TFEs.If our recommendation to allow TFEs for all requirements is not viable then the following requirements should allow an entity to request a TFE. (R5, R6, R8, R9, R10, R13, R14, R15,

#	Organization	Question 53 Comment
		R16, R17, R18, R19, R21, R22, R23, R26)Example justifications are as follows:R5: BES Cyber Systems where physical security cannot reasonably be provided such as devices that are physically hung on a transmission line such (i.e. transmission line fault detectors). R6: While physical protection of the physical security systems should be feasible in most instances, there may still be instances where mitigation measures need the oversight provided by the TFE process.R8: The majority of substation devices use the concept of "shared" accounts. While an entity can add a device to facilitate logging into substation devices, there is not a feasible way to "monitor" these accounts on the purpose built devices themselves such as protective relays. R9: Depending on the method chosen to physically protect the BES Cyber System, it may not be technically feasible to revoke physical access to every location within 24 hours for an individual terminated for cause if an individual does not return their key (physical key, electronic key, or otherwise).R10: There are numerous examples of legacy devices which cannot meet the requirement of a 6 character password, or a password with special characters, etc.R13: Depending on the method chosen to electronically protect remote access to the BES Cyber System, it may not be technically feasible to revoke remote access to every location within 1 hour for an individual terminated for cause if an individual does not return their key (physical key, electronic key, or otherwise).R14: There are rare instances where remote access may be needed without 2-factor authentication such as for the administration of the device that authenticates the remote access itself. There are also instances where a display of appropriate use banner is not technically feasible.R15: While this requirement should greatly reduce the number of TFE's submitted based on the existing CIP v3 malware requirement, there will still be existing legacy purpose built BES Cyber Systems that do not have the ability to detect and respond to the introduction of malicious code. Specifically, consider the case of a protective relay with no external connectivity.R16: The allowance for TFE's should carry over from the existing CIP-007-3 R3.R17: Based upon the existing TFE framework, the language "shall document and implement a mitigation plan" from row 17.1 would necessitate that a TFE be filed.R18: There exists no such tool or process to monitor for system events related to cyber security on protective relays with no external connectivity.R19: Not all data protocols include a checksum. Whereas most SCADA protocols do contain this data error detection functionality, this requirement (19.1) is not limited to those inbound SCADA connections. There are a number of reasons, supported by the DHS Catalog of Control System Security itself, where an entity may choose not to encrypt all data inbound to a BES Cyber System (19.2).R21: There may be shared

#	Organization	Question 53 Comment
		cyber system components between BES Cyber Systems that do not provide logical separation. Clarification of this requirement may resolve the need for a TFE allowance on R21.R22: The TFE allowance justification for R22 carries over from the justifications for R14, R16, R18, and R23.R23: There are a number of devices for which there exist no such tool to monitor changes to the baseline configuration (23.7). In addition, it will not be feasible to monitor and detect changes for those systems with no external connectivity.R26: There are maintenance devices for which there are no known methods to detect and prevent the introduction and propagation of malicious code. Examples include devices such as data analyzers, birdogs, etc.
53.61	Constellation Energy Commodities Group Inc.	We support the effort to reduce the need for TFEs; however, the complexity and variability of systems across industry make it difficult and inappropriate to expect one-size-fits-all requirements.The password complexity requirements should either be written so as to avoid the need for TFE's, or clarified to specify that the use of maximum complexity allowed by the device is sufficient.
53.62	Entergy	Where the need for TFE has been obvious to us we have noted as such in comment to the respective requirements. We will be more thorough during the formal comment period.
53.63	Con Edison of New York	Will Technical Feasibility Exceptions still be accepted, required or will this process no longer be enforced? The Password requirements would still drive the need for TFE's. TFE's may be avoidable if the standard allows for internal documentation and approval of exceptions. There will be many TFE required because the net has been cast on so many different unique type systems that are located on the power system. Many of these systems are 20 to 30 years old. The CIP is written to address concerns for new technology computer network systems. Much of the equipment used on the power system is uniquely built and not designs with a full wide area network design.It would be a much better approach to address the SCADA systems (remote control and indications) & EMS systems and pay less attention to trying to force all the other unique (less critical) equipment in the same square hole.

54. Do you have any other comments to improve this version of draft standard CIP-011-1?

Summary Consideration:

Many of the commenters stated that the Standards need additional clarity. Define what is meant by words like monitor and review and remove potential ambiguity. Make clear the intent or objective of each requirement. The timing requirements of the standards need to be clearly defined. In response to these comments, the drafting team has made several steps to improve the clarity of the standards. These steps include moving to a Results-Based Standard approach, where the reliability objective must be specified for each requirement. Also the Drafting Team reviewed these standards with regional CIP auditors, with FERC, and with industry representatives ahead of the NERC Quality Review process to gain additional clarity in the requirements. The Drafting Team agrees and has made efforts to eliminate inconsistent terms and phrases and to consistently and unambigouously use timing phrases throughout the standards.

Commenters stated that the Implementation Plan should address the significant amount of effort required to comply with the standards for the many new cyber systems that will be in scope. Significant time should be included in the Implementation Plan for the categorization of BES Cyber Assets and for the transition from previous versions of the CIP standards to the Version 5 standards. The Drafting Team is proposing to allow 2 years for the Responsible Entities become compliant with all of the CIP standards and to allow entities the option to become compliant earlier if they choose to bypass Version 4 compliance.

Many commenters expressed a common theme to remove or minimize requirements for Low Impact BES Cyber Systems. Since the overarching objective is to provide for some level of security for all BES Cyber Assets, the Drafting Team has kept the requirements for physical and electronic boundary protection as well as basic security program elements such as policy, awareness and incident response, for the Low Impact BES Cyber Systems.

#	Organization	Question 54 Comment
54.1	Independent Electricity System Operator	- Specify calendar or business days when referring to a time frame- Issue with the bundled approach-- if you violate more than 3 in the same standard, this affects the VSL? need to look at NERCs governing procedure on VSLs- Strongly suggest that standards
54.2	Consultant	1. Each requirement should have a unique title. Currently the requirements are grouped by the subject area, but the requirements typically are just a statement. This makes it difficult to reference requirements except by number. What will really happen is everyone will develop their own "short title" for each requirement number, and it will not be consistent across the industry, and will result in

#	Organization	Question 54 Comment
		confusion.2. There should be consistency for the requirement title, the associated table name, & the requirements column heading for each requirement. Currently these three items are not necessarily consistent, and in some cases there doesn't seem to be a connection or relationship in the terminology in these locations.3. If the Requirements Groups are going to stay in the standard then they should be numbered in order to facilitate cross referencing the groups.4. The word "criteria" in the requirement statement should be change to "requirements" where it occurs. The tables list requirements, not criteria. (Multiple instances throughout CIP-011)5. There is different sentence structure and grammatical structure throughout CIP-011. While it is a good idea to combine the requirements in a single standard, it still appears to be written by multiple authors. There are still access control and account management requirements scattered across multiple requirement groups, and each is a bit different. Another example, the incident response and the recovery plan requirements groups should be very similar, but are, in fact, very different in the requirement and the wording of the requirements, much like the differences noted in CIP-008 and CIP-009. The structure of the "local definitions" is different throughout.Suggest a "wide area" review to make the standard appear to be written by a single author rather than multiple authors.6. The definitions should be written as definitions. [Defined Term - Definition statement.] The wording "for the purpose of this standard" is not correct, and thus unnecessary. The glossary collects definitions from the standards when the glossary is updated. The next update should add the terms defined in these standards, and therefor they are not "for the purposes of this standard". Also, the words "is defined as" are redundant as it is a definition.7. Data retention requirements should be included as requirements. Moving data retention to Section D isn't logical. If there is no requirement for data retention, then it isn't a viable compliance activity. At the workshop it was stated that this was a NERC format. In this case NERC is wrong and needs to correct the format, both for these standards and for the other reliability standards. 8. Suggest dropping all requirements for assets categorized as Low Impact. They are after all, low impact on the BES. Based on the discussion at the workshop, looking at a 10 year implementation timeline for low impact assets is effectively the same as no implementation. Many things will change in 10 years, and expenditure of resources in the low impact is unlikely to have any increase in BES security. The Low Impact category needs to remain as part of the categorization process in order to include all BES assets in that process.9. There are multiple requirements that differentiate between types of facilities in the requirements tables. This is an indication that the categorization criteria is incomplete or incorrect, or

#	Organization	Question 54 Comment
		that the requirements are not properly stated. If a requirement currently indicates in the High Impact column that it applies to Control Centers only, then either (1) the transmission, generation, and special systems are not "High Impact", or (2) the requirement statement doesn't properly address all asset classes.The categorization criteria should properly place each asset in each asset class in the appropriate category with "bright lines" to eliminate adding categorization in the requirements.10. While this format for commenting and collecting comments seems good, there should be a mechanism to complete the form 'non-sequentially'. For example, as comments are made through the form's current sequence, if a 'general' comment arises, the only method to enter that comment is to page through to the end, save the comments, and then reopen and page back to the location where you started. This is not very user friendly.11.The commenting tool should have a "Save and Continue" option to allow saving work in progress without exiting and re-entering the tool.12. An improvement to the "status bar" of the commenting tool would be a table of the questions with an indication for each question if a response has been entered.
54.3	Con Edison of New York	A few general questions:Will there be an implementation plan? The document for comments indicates there will be an implementation schedule that will take into consideration existing BES Systems (CCA's) and newly defined BES Systems (CCA's). In order to be able to meet the requirements in CIP-011, the devices on secured networks that are not currently CCA's by definition but are "treated as" since they are on the same network need to be considered as part of the implementation plan. The inheritance rules may require newly defined CCA's in order to allow the time that we be needed to address these additions. If they are considered existing since they are "treated as" a short implementation period could be an issue.Is there a six-wall physical boundary requirement in this version of the standards? Suggested additional defined terms:"BES Cyber System Failure": should be defined to serve as shorthand for the long list of items currently used in the draft CIP-010/011 Reliability Standards.Current Wording: "disruption, compromise or failure of BES Cyber Systems""if destroyed, degraded, misused or otherwise rendered unavailable"Proposed Wording:The term 'failure' when used in conjunction with the terms BES Cyber Component and/or BES Cyber System shall encompass the meanings 'malfunction, disruption, compromise, failure, destruction, degradation, misuse or unavailability' of those.Suggest replacing term "affect" with already defined term "adverse reliability impact". The drafting team (DT) uses the terms "affect" and/or "affects" without providing any specific meaning, system impacts, or other bounding explanation to describe that term. Proposed

#	Organization	Question 54 Comment
		Alternative Wording:NERC Glossary of Terms - Substitute definition for BES Cyber System "affect" or "affects." [Causes] Adverse Reliability Impact - The impact of an event that results in o frequency-related instability; o unplanned tripping of load or generation; or o uncontrolled separation or cascading outages, that affects a widespread area of the Interconnection.
54.4	Allegheny Energy Supply	A lot of work went into the prepration of the existing CIP-002 through CIP-009 standards. This new CIP-011 standard completely throws away that body of work in favor of this new approach. While there are many good things about the new approach, please consider the amount of work that entities have given to helping to refine the CIP-003 through CIP-009 drafts and to create and implement the current compliance plans and related software systems. We suggest that you consider incorporating the new ideas as incremental changes to the existing standards. It would be helpful for the drafting team to develop additional documentation providing more information about the threat basis that the standard is intended to provide protection against. The opportunity is to inform asset owners/operators of how and where to prioritize efforts to protect components of the BES.Suggest that the standard require physical security controls for BES Cyber Systems that no more stringent than other requirements for the BES equipment that the BES Cyber System controls, protects, or monitors.Suggest that the standard require controls that are commensurate with the amount of risk of compromise that a device presents. Not all BES Cyber System components face the same risk, or if compromised, have the same potential impact on the BES. For example: - Serially attached electronic components do not face or create the same risk as those that use routable protocols. - Devices that communicate to each other within a self-contained, isolated network segment (for example within a substation) do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.- Devices that use dedicated (and non-routable) point-to-point communications channels do not face or create the same risk as devices that communicate via routable protocols across multiple geographic or logical boundaries.
54.5	Allegheny Power	Allegheny Power does not understand the need to eliminate and combine CIP-003 thru CIP-009 into a new standard CIP-011. AP believes that the objectives of the Standard Drafting Team to provide further clarification and remove the uncertainty of the current CIP standards are proper and necessary. However, AP believes that these same objectives can be accomplished by incrementally revising the current CIP standards and not force changes in terms, concepts and numbering schemes

#	Organization	Question 54 Comment
		which would essentially force all entities to start their CIP compliance efforts over from the beginning. AP would like the SDT to abandon the concept of completely rewriting the CIP standards in favor of incrementally revising the existing standards to accomplish the same objectives.
54.6	Lincoln Electric System	Although much of the standard seems very practical, LES believes it was written with routable systems in mind. When applied to systems with only non-routable connections, or even no connections, many of the requirements are not very applicable, and would set the stage for numerous TFE's within the industry. LES believes this either needs to be addressed requirement-by-requirement, as in the approach taken by the MRO NERC Standards Review Subcommittee (MRO NSRS), or there should be a blanket statement that removes non-routable systems from the requirements that are not applicable. Either way, LES believes this differentiation is extremely important, since non-routable connections (or even better, no connections) are inherently more secure against, and limit potential damage from, remote attacks, and by default eliminate the threat of propagating localized attacks to other facilities.
54.7	Oncor Electric Delivery LLC	As the tables of CIP-011-1 specify certain requirements for "Control Center Only" or "External Connectivity", the additional requirement of "Routable Communication or Dial-up Only". Many requirements do not even make sense without integral communications being part of the cyber systems. If there isn't communication involved, the cyber system should be excluded from a requirement.
54.8	Garland Power and Light	At the CIP workshop, there were several comments that were made that were "depends" or "our intent was" o The "depends" requirements need to be reworded so that requirement is clear. o The "intents" need to be expressed clearly in the document because it is almost guaranteed that the will be many different interpretations if they are not expressed.
54.9	Constellation Power Source Generation	At the workshop, it was stated that an assumption of the SDT that High Impact BES Cyber Systems were most likely already Critical Cyber Assets per the older standard. This is false. Non routable protocols and other criteria used by Registered Entities have excluded certain assets at critical locations from being critical cyber assets. A 3 year timeframe should be implemented for High BES Cyber Systems to be fully compliant if it was previously not classified as a CCA. Another suggestion for implementation is to make the procedural requirements auditable first, and then implementing the

#	Organization	Question 54 Comment
		other requirements in stages. Furthermore, as stated in the workshop, allowing an entity to declare advanced implementation for audits would be of great benefit, as compliance with the new standard will take years to implement. The blank boxes found in the requirements tables of CIP-011 are implying that a high/medium/low BES Cyber System does not need to comply with that requirement's particular control, but that is not written anywhere. A blanket statement in the beginning of CIP-011 needs to state that the intent of an empty box to avoid confusion. An audit standardization or guidance document should be developed for use by auditors/reviewers of compliance to NERC CIP standards. Even though the formalization of cyber protection compliance programs are relatively new within the NERC standards body, there are mature examples of cyber protection and information security controls frameworks comprised of formalized cyber security standards, compliance management methodologies and auditing guidance such as defined in NIST 800-XX and ISO 2700X regimens . These regimens include guidance and standardization for auditing compliance (e.g., NIST SP800-53A). Other examples of formalized auditing guidance include guidance documents published by ISACA (Information System Audit and Control Association). These regimens include formal auditing guidance to ensure comprehensive coverage of compliance requirements, consistency in auditing approaches and better insight for auditees in ensuring auditability for their compliance audits. This improves the effectiveness as well as the business efficiency of companies' compliance programs. This rationale also applies to the NERC CIP program.
54.10	E.ON U.S.	Because Distribution Providers are for the first time made subject to CIP standards they may need additional time to come into compliance
54.11	ReliabilityFirst Staff	Because the acronym "BES" is not included in the NERC Glossary of Terms, we suggest that BES should be spelled out in the Introduction to this standard.
54.12	Reliability & Compliance Group	By dividing up the Standards and just revising CIP-002 through CIP-009, it makes it easier for the Registered Entities to update their existing documentation. It allows for the creation of a "crosswalk" document that helps examine the changes. While it may not be able to be done requirement by requirement and sub-requirement by sub-requirement, it can be done Standard by Standard. Where possible, it would be good to create a change crosswalk document that lists the version 3 requirements and the points to where they are now covered in the version 4 standards and note that

#	Organization	Question 54 Comment
		there is either a major change or a minor change.
54.13	LADWP	CIP-011-1 R16 The patch management does not specify a required time for installation of patch. The entity should be given the ability to determine the schedule as systems vary on when they can be brought down to install a patch. The language in R16.2 addresses the issue and no additional language to restrict the installation time needs to be included.
54.14	City Utilities of Springfield, Missouri	City Utilities of Springfield, Missouri supports the comments of the APPA Task Force.
54.15	US Army Corps of Engineers	Definitions within the standard need to be improved so they are less ambiguous.Statements like those found in Table R21, 22.1 "Cyber system components that provide external communication to the BES Cyber System must only communicate externally through an electronic access point as specified in Requirement R20", are confusing. What is the standard trying to say here?
54.16	USACE HQ	Definitions within the standard need to be more direct and narrower scope. Also, the relocation of all of them to a separate attachment would help too.
54.17	Dominion Resources Services, Inc.	Dominion recommends placing all requirements into a requirements table. It is sometimes difficult to distinguish requirements mixed into the preambles.Using a single standard for all requirements is preferred; however the format internal to the single standard is inconsistent. For example, some requirements are in paragraph form while others are embedded in a requirements Table. All requirements should be contained within a requirements Table. Where possible, information preceding the table should be used only to state the context and establish the security objective or intent behind the requirements.
54.18	EEI	EEI would like to thank the members of the Drafting Team for their significant efforts on this important issue.
54.19	Black Hills Corporation	Emergency Response: Emergency Response provisions are limited to R3 & R4, and address training and risk assessment controls. There are many possible scenarios that could be identified which would

#	Organization	Question 54 Comment
		require emergency exceptions to most of the requirements of CIP-011. There should be a general emergency clause that allows appropriate response to many possible emergency situations.Outside Vendors: There is no mention in the rules how the use of outside vendors should be addressed. A common solution could be to have the responsible entity extend the necessary requirements of these regulations to the third party via contract. (Example from other regulatory efforts includes the HIPAA regulations and their business associate requirement). An example of this in action could be the requirement that a contractor conduct the personal risk assessment, according to the requirements specified in CIP regulations.
54.20	Exelon Corporation	Exelon companies have embraced the development of logical, clear and effective reliability standards as evidenced by its commitment of time and resources to various standard development initiatives (including participation on several NERC and Regional Committees, Sub-Committees and Standard Drafting Teams). As evidence of our commitment, Exelon has devoted in excess of 4 years and $11 million for the implementation and integration of the NERC CIP-002 to CIP-009 Standards. We have concerns with several aspects of the CIP Version 4 Standards. The CIP Version 4 Standards represent a significant change in the scope of the standards in the equipment/systems that fall under the standards as well as the elimination of terms/categories of assets. Exelon is also not in favor of changing the current CIP-002-009 standards to the new CIP-010 and CIP-011 format.. Each change in itself represents a significant “change management” issue that impact databases used for the tracking/storing of evidence of compliance, training requirements, safeguards, and systems that have been put into place to ensure Exelon’s continued compliance to all NERC Standards. Exelon feels strongly that the proposed changes must be accompanied by a risk based analysis as justification for such dramatic and costly changes which to date have not shared with the industry. Essentially we are most interested in understanding the incremental difference or benefit of moving away from the current Regulatory approved CIP-002 to CIP-009 standards to a different set of standards that will result in many of us “starting from square one” to implement. Policies, procedures, contracts, training, drawings, methodologies, systems, data structures, and countless other documents will need to change to reflect the new language and concepts. The confusion that this will cause within organizations to retrain personnel and realign around the new standards cannot be underestimated. In fact, Exelon may even need to put some value-added compliance projects on-hold because the entire design will need to change with the implementation of the new standards.Specifically, Exelon

#	Organization	Question 54 Comment
		would like to see the SDT: Discard the concept of a wholesale rewrite of the CIP standards -- but use the standards drafting team work as an input to the process. Incrementally change the existing CIP-002 through CIP-009 standards to clarify and improve upon the established approach. Retain the fundamental terms, concepts, and standards numbering scheme to enable continuity.This approach would more effectively build upon the work that has already been accomplished, while allowing the industry to continue to improve on security and compliance related to critical infrastructure.Compliance with NERC cyber security standards should be re-scheduled for nuclear generation. That is, nuclear generation is currently in the process of compliance with Version 3 of CIP-002 thru -009 by September, 2011. However, it appears that compliance with Version 4 of the standards may be required by 2013. In terms of resource expenditures, ultimately borne by consumers of electricity, it seems wasteful to build a program for nuclear generators based on CIP-002 thru 009 that will be scrapped roughly two years later to be compliant with CIP-010 and CIP-011. Such scheduling will result in maintenance of a program based on CIP-002 thru -009, including audit support, and purchasing and installing equipment during refueling outages, at the same time a new program built on CIP-010 and -011 is being constructed. This new Version 4 program will include doing away with the concept of Critical Assets so that purchase and installation of the equipment previously installed may no longer be required. The existing cyber security programs and regulations in place or in process to protect nuclear generators, e.g., NEI-04-04 and 10CFR73.54, the limited contribution of nuclear generation to the BES (roughly 20%), and the limited time until Version 4 of the NERC Standards are expected to be in force all limit the cyber vulnerability of nuclear units. It is recommended that the implementation of Version 3 of CIP-002 thru -009 for nuclear units be deferred, and compliance with NERC cyber security standards for nuclear generation be re-scheduled for Version 4.
54.21	BGE	General - The wording was changed to “at least every 12 months” instead of “annually” in previous CIP versions. Can the exercise or test occur in the same month each year or must it be 11 months 29 days or less from the previous exercise/test?
54.22	Network & Security Technologies Inc	Good start! Strive for clarity. Ask both individuals responsible for compliance and auditors for their interpretation of every requirement. Be explicit about what’s required (e.g., documentation of, records to demonstrate compliance with, etc.). It’s okay to not be very prescriptive but try to avoid

#	Organization	Question 54 Comment
		implied requirements - they will be a source of endless debate.
54.23	CWLP Electric Transmission, Distribution and Operations Department	Guidance documents should be available before balloting these standards. All terms used should be defined in the NERC Glossary of Terms or in the standard.
54.24	Green Country Energy	I really like the way the standard is developing it is a huge improvement and hopefully with industry comments it will develop into a fine standard that meets everyones expectations.I would like to see a Guidance Document, footnotes, measures and VSLs etc to make compliance and auditability a lot clearer and less subjective.
54.25	US Bureau of Reclamation	It seems that the standards are applying a postage stamp level of security to Cyber elements involved in BES reliability. Multifunction relays or Solid State relays which are programmable must now have eletronic access attributes which are normally associated with BES computer control systems. The SDT should reexamine the true nature and scope of these types of systems before lumping these deviced together with traditional computer control systems. Lumping everything into one standard will make adminstration by the Responsible Entities and Reliability Entities difficult and may add to confusion with respect to individual table elements.While the tables applied to requirements in CIP-011 are an excellent way to establish security requirements for the 3 levels of system impact addressed, the empty fields should be avoided as they lead to confusion on the part of readers. All blocked fields should indicate something, even if it is an indication that the requirement is “Not Applicable,” “Not Required,” “Addressed under Requirement xx.x, above,” or “In accordance with entity policy.” Further, all requirements should include the 3-level requirement application table, even if the requirement applies equally to all three levels. This will further avoid confusion when reading the Standards.Appreciate the “blocked-out” area-specific definitions, but the drafting team must ensure that this feature is only used for area-specific needs and not global definitions. If the scope of the definition extends beyond a specific section there could be problems with sub-dividing the document to simplify what is handed over to organizational components with different functional responsibilities, particularly if the definitions do not also appear in the NERC glossary.The use of “objective statements” is very much appreciated, both as a guide to entities addressing

#	Organization	Question 54 Comment
		implementation and also (we would assume) to reviewers and audit staff addressing compliance. We encourage the drafting team(s) to continue this direction and to strengthen and refine the objective statements in order to provide clear direction for Standards users, including down to the sub-requirement level (as applicable).
54.26	Luminant	Measures need to be defined
54.27	Minnesota Power	Minnesota Power believes that, for all requirements which specify that something must be completed within X hours, the Standards Drafting Team consider using the following statement:"As soon as practical, but not exceed x business days from the date reported."This would preserve the spirit of the requirement, but also allow for more practical time frames.With so many auditable elements included in these Draft Standards, Minnesota Power believes that the VSL's cannot be written with the current zero-defect mentality. It would be more practical to allow for minor issues to be identified and scheduled for corrective action without representing immediate non-compliance which will result in extended investigations and settlement proceedings.Minnesota Power recommends that the Standards Drafting Team consider using a technical writer and/or solicit feedback from multiple proofreaders who have not been involved in the creation of this Standard to ensure that the following items are addressed: o any interpretable vocabulary is defined o grammar is correct o punctuation is correct o meaning is clear and does not require any guessing as to the intention of the Standards Drafting Team.This should be done prior to the official comment period, so that the Industry can concentrate on technical aspects of the review, rather than spending time on interpretation. The ability of Registered Entities to properly interpret the Requirements is highly dependant upon clear wording, good grammar and proper punctuation. This has been one of the greatest problems with the version 1 through 3 CIP standards. Minnesota Power requests that the Standards Drafting Team ensure that improper writing does not change or hide the intended meaning. The misuse of
54.28	Progress Energy (non-Nuclear)	More examples of requirement application to the real world would aid auditors and the industry.In CIP-011 If the record keeping and retention for compliance is similar to previous standards this standard significantly increases the record keeping administrative burden on utilities and compliance authorities due to the number of devices which are now to be declared without actually increasing security of BES.Implementation plan (when developed) needs to consider how it will overlap existing

#	Organization	Question 54 Comment
		standards compliance record-keeping and documentation, then establish a phased-in approach of the new standards to eliminate double record-keeping and double documentation across audit compliance periods.Implementation schedule needs to be developed that allowsHigh - 4 yearsMedium - 4 yearsLow - 4 yearsNeed clearer definitions of annual, quarterly, etc.Need to resolve issues/questions with current standards:How is communication/wiring covered by the standards? This becomes even more of a question when a BES Cyber System could be defined as a SCADA system including all of the RTU's which support it.Within ESPBetween ESP'sInto/Out of ESPPassword strength/management. Improvement has been made here, but it is still not clear if requirements must be enforced by the assets in question or if policies are sufficient. For instance, regarding the requirement to change passwords at least once every 12 months, must the device force this password change, or is it sufficient for an entity to have a policy requiring compliance along with documentation to attest that the policy was followed?Timeframe for revocation of access for expired training/background checks. NERC CIP Training is required at least every 12 months. It can be assumed that if the training is not completed in the allowed timeframe that access must be revoked; however, it isn't clear if this revocation must be done immediately, within 24 hours, 36 hours, 72 hours.There is currently no provision for moving cyber systems from one ESP to another (such as between a primary and backup ECC). Although this type of even will need to happen from time-to-time, it is left up to each entity to determine how that can be accomplished within the standards.There is no clear distinction between various types of Access control. It is obvious that the standards apply to network facing logins for BES Cyber System Components;however there are other types of access that are not clearly addressed or excluded such as-Access to configuration controls for something like a time standard which are only available to someone with physical access to the front of the device-Access to the BIOS on a typical PC-Access to various functions/programs on a machine - some of which may require special login - others which don't.How 7 year background checks are handled for someone under the age of 25 since juvenile records prior to the age of 18 may not be legally searched in many cases.Will the TFE process continue? What a TFE is, where it is/is not allowed, how it is to be handled (regarding documentation, approvals, submittals, periodic reviews, etc)
54.29	Michigan Public Power Agency	MPPA is concerned with how these standards would impact its members who are registered entities but do not own or operate facilities that are, by NERC definition, a part of the BES. MPPA recommends clarification in the applicability section with the insertion of ", that operates BES facilities,

#	Organization	Question 54 Comment
		" between "...Functional Entities..." and "...will be collectively...". This segment of the sentence would then read as: "...Functional Entities, that operates BES facilities, will be collectively..."
54.30	ISO New England Inc	Need more precise, well-defined language. Several requirements are measures, not standard requirements to measure against. Provide examples, FAQ, what is the actual risk/ driving requirement - what are we trying to protect against? Understanding the background to the requirement will help to define defenses to perceived threats that this standard is trying to protect. Clearer definitions of Cyber Systems, Cyber System Components, Control Center. Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional pageRequest that the tables and time constraints be consistentEliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (see R5-R32)Request a cross-reference of CIP-011 Requirements that refer to another CIP-011 Requirement - especially the Access Control Requirements. Diagram might help.
54.31	WECC	Need to have consistency in spelling out time periods versus numerically showing them (ie thirty-six months vs 36 months). Also need consistency in use of the tables as some say "criteria" and others say "procedures" or "processes". In many cases when a requirement states that you should have a process or a procedure it might be easier for audit purposes to instead require a program that addresses many of the processes or procedures required. A single requirement for a program or plan that meets a table of criteria might reduce the number of requirements and ease audits. For instance "Wireless Security Program covering the following risks" "Remote Access Program addressing the risks in Table X" "Maintenance Program addressing the criteria in Table X" "Physical Security Program addressing the criteria in Table X"
54.32	US Army Corps of Engineers, Omaha Distirc	Next draft should include the measurement criteria. Standards are very computer center centric.
54.33	Regulatory Compliance	NRG Energy Inc. is concerned with some of the impact criteria in Attachment II related to transmission and generation Facilities. To base impact on "bright line" Facility Rating thresholds, i.e., MW, kV, MVAR, etc., could lead to mis-categorization and ultimately unprotected cyber systems. These thresholds do not take into consideration regional differences in configuration and load flows.

#	Organization	Question 54 Comment
		Therefore, it is our suggestion that categorization could be based on the results of a regional engineering study, similar to what is currently required in the TPL Standards. This study could be conducted by the regional Planning Authority(s) or an independent third party and approved by the Regional Entity. The results of the study would identify the contingencies that have the potential to cause the following levels of impact to the BES: Â· High Impact (has the potential to cause an Adverse Reliability Impact) Â· Medium Impact (has the potential to require planned/controlled loss of load) Â· Low impact (has no potential to cause loss of load)
54.34	National Grid	o There is inconsistency in using “processes” or “one or more processes” in several requirements. For example R25 states that Each Responsible Entity shall document and implement one or more processes...” while R26 states that Each Responsible Entity shall document and implement processes...”. National Grid recommends using “one or more processes”. o Request that the tables and time constraints be consistent o Eliminate confusion caused by two 3.1’s. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (see R5-R32) o Request a cross-reference of CIP-011 Requirements that refer to another CIP-011 Requirement - especially the Access Control Requirements. Diagram might help.
54.35	Southwest Power Pool Regional Entity	Overall auditing issue: The requirements need to consider issues of sufficiency (adequacy of the entity solution) without being prescriptive in the solution. Where possible, clearly define the objective and do not prescribe technical solutions. Also, avoid the use of adjectives in defining the objective and / or specific requirement. Terms such as “adequate”, “sufficient”, and the like are very difficult to objectively audit. Overall observation: The implementation plan concept presented at the May 19-20 workshop in Dallas, coupled with the proposed applicability matrix for Medium and Low impact BES Cyber Systems will likely reduce, not improve the overall cyber security protection afforded the BES Cyber Systems today. A good number of existing Critical Cyber Assets will fall out of the High impact category, many becoming Low impact, with the resultant relaxation of protections. The applicability matrix as it appears today does not define a reasonable baseline of protections for Low and Medium impact systems. Re-categorization of BES Cyber Systems: While this will hopefully not happen very often, a BES Cyber System that sits on the cusp between two categories could find itself being re-categorized more than necessary unless some sort of a dead-band is introduced that would preclude re-categorization as a result of a small change. Implementation Plan: There needs to be a consistent

#	Organization	Question 54 Comment
		implementation plan for any BES Cyber Systems represented under today's standards as Critical Cyber Assets regardless of their ultimate categorization. Any existing Critical Cyber Asset should be afforded a very short timeframe to achieve compliance under the new standard(s) as it can be reasonably be expected to be already compliant. This is similar to the Table 1 entities concept for Version 1 of the existing standards where entities subject to the UA 1200 standard were given the shortest timeframe to comply. Consideration needs to be given to how an entity will migrate from compliance with the existing standards to the new standards. A piecemeal approach will be very difficult for the entity to maintain and for an auditor to evaluate compliance.
54.36	Alliant Energy	Per previous comments, all occurrences where prescriptive timeframes for removal of access are based on a complicated combination of impact level and BES Cyber System type. This level of complexity adds confusion and undue administrative overhead in situations of job change, which would cause low risk to the BES. Recommend a solution that provides consistent timeframes based on the cause of the business need change. Terminations for cause should remain at 24 hours for all removals of BES system access. Other changes in business need should allow for processing over extended holiday weekends without being treated like an emergency response. These changes should remain at 7 calendar days. Any distinction between low, medium, and high impact BES Cyber Systems should be made in the wholesale application or omission of this requirement. Per previous comments, all instances where 12 calendar months are used as the outside allowance for renewal a rolling creeping calendar is introduced. Recommend changing all 12 month timeframes to either 13 calendar months or 5 calendar quarters from the previous completion to allow entities to maintain a program with an annual training rollout with the appropriate amount of lead time to be successful in annual renewal. A 12 month timeframe will create a training program that becomes administered on a user by user, day by day basis without considerations for consistent annual content updates and bulk annual renewal.
54.37	FirstEnergy Corporation	Please see our response to Question 1 for the FE Summary view of the proposed CIP V4 standards.The new format, tables, information boxes is a good change o We question whether the new format (low-to-high impact, in particular) will encourage us to categorize more as high so we track things in a similar way. It seems like an administrative burden to try to track things at three levels. It is hard enough to track everything now with just one level. This 'administrative burden' issue crops up in

#	Organization	Question 54 Comment
		several places.
54.38	PacifiCorp	Procedural exceptions are onerous to manager operationally; the standards would be more effective if less differences in revocation of access were implemented across the BES system and criteria.The term "Annual" is not defined. "Annual" requirements were changed to 12 months in most cases (not consistently). The 12 month requirement causes "schedule creep". Define "Annual" in the NERC glossary to be 12 months not to exceed 15 months. Change all 12 month references back to "Annual" or, preferably, use the definition of annual defined for the NERC FERC Standards of Conduct (calendar year). The following FERC Directives need to be addressed with version of of CIP-010 and CIP-011: o 2 or more diverse security measures for defense in depth at the security boundaries o Active vulnerability assessments every 3 years o Incorporate forensic data collection and proceduresThe framework is in place to incorporate requirements in CIP-011 that address the directives. CIP-011 has a potentially long implementation time. FERC will likely not wait for the implementation of CIP-011-1 to be complete prior to making NERC address these directives. Incorporating these directives in the middle of the implementation of CIP-011-1 will be confusing and cause additional expense and effort. Don't wait. Address the following FERC Directives in version 1 of of CIP-010 and CIP-011.
54.39	Southern California Edison Company	SCE recommends revising the numbering of CIP-0011-1. Between CIP-010 and CIP-011 the drafts should indicate the intention of the intent is to retire CIP-002 through CIP-009 then it would make more sense to call these standards CIP-002-5 and CIP-003-5 with CIP-004 through CIP-009 being retired. Otherwise, the gap of unused numbers between CIP-001 and CIP-010 will potentially cause confusion. SCE also suggests rearranging the structure of these new requirements. for example, by breaking up CIP 011 into functional areas such as Governance & Personnel, System Security & Boundary Protection (with Incident response since “incidents” are cyber security incidents), Access Management (Physical, Electronic and Information), and Disaster Recovery Planning & Capability. From a policy formulation perspective, this would result in fewer policies than CIP 011 as it is currently structured. For example, combining physical access controls with electronic access controls provide the means of utilizing a combination of both to determine sufficient total security. Providing secure physical access controls and disconnecting routable communications such as gateways and/or modems.Finally, separate and apart from the recommendations made above, SCE also recommends allowing use of local definitions as in-line guidance at the requirement level. The use of local

#	Organization	Question 54 Comment
		definitions in addition to the NERC glossary is good approach. The text of each requirement objective should be such that it is only a objective and not a control statement. A control should reside within the impact level table. For instance, R11, R12, R18 contains control statements within the objective.
54.40	San Diego Gas and Electric Co.	SDG&E notes that it appears the drafting team took the approach of defining the details and then working up to the bigger picture items, i.e., BES Cyber Systems Component to BES Cyber System. SDG&E feels that there is risk associated with taking this "bottom up" approach to the standard setting process vs. the "top down" as used in the previous three versions of the standards. The risk is that components posing no significant risk to the BES system can get "swept up" into BES Cyber System definition and require protection commensurate with components that are correctly required to have strong security measures.SDG&E feels that part of the issue with Versions 1-3 of the CIP standards was that the "top down" approach to critical asset identification was not started high enough; it was started at the Responsible Entity level rather than at the Region / Reliability Coordinator level. If that level is deemed too high, even a sub-region level would be more appropriate. In SDG&E's case, it has a view of its assets in the context of its service territory that serves 1.4 million retail customers. Independent generators on the other hand don't have that regional view. In Southern California, for instance, congestion is high in some places and regulatory mandates for incorporating renewable energy are growing. Thus, the risk to the BES can only be fully evaluated when considering sources (generation - fossil and renewable) and uses of energy (load) in the region as well as the adequacy of transmission to balance and move power. In such a scenario, the assets critical to BES stability and/or restoration are much easier to identify and so too are the BES Cyber Systems that support them. For those entities that do not have a region or sub-region view, perhaps the Regional Entity, Reliability Coordinator or Balancing Authority could be responsible for identifying which assets are critical.
54.41	Manitoba Hydro	Section D Compliance: 1.4 Data Retention should include all documentation, inventories, logs, etc that are mentioned throughout the Requirements, or include a "catch all" requirement for data retention for all other documentation referenced by the Requirements.General Comments: The language in Requirement R1 indicates that each Responsible Party shall "develop, implement and annually review one or more formal, documented cyber security policies" addressing the listed Requirements. This should be clarified to confirm whether a formal written policy is required for each of the listed Requirements or only for selected Requirements. From the language of the specific Requirements one

#	Organization	Question 54 Comment
		could assume that those Requirements that indicate "document and implement" require the Responsible Entity to prepare a written policy/process of some kind, while those Requirements that indicate only "implement" do not. Then there are those Requirements that require the Responsible Entity to "create, document and implement" - it is not clear if this would require something different than "document and implement". There are also those Requirements that simply require that certain criteria be applied which would seem to indicate that no documentation is necessary. If the Responsible Entity is to assume that the Requirements that indicate "document and implement" require the Responsible Entity to prepare a written policy/process of some kind, it is assumed that there may be one master policy covering all elements of the Requirements that must be documented given the language in Requirement R1 "one of more formal documented cyber security policies" and that separate documented policies for each of the Requirements requiring documentation are not necessary. Certain references to "review" in the Requirements should be clarified to indicate on what basis the review is to be conducted, what criteria should be applied, what the Responsible Entity should do with the results, etc. i.e. Requirements R5-5.6, R12-12.1, R18 -18.4. The same comment applies for certain references to "monitor" (i.e. Requirements R8-R8.3) and "verify" (i.e. Requirements R24-R24.5). Where no review or monitoring of developed protections or processes is specified, is it to be assumed that no review or monitoring is required? (Requirements R15 and R16) Each of the Requirements seems to provide a reason or justification for their inclusion i.e. Requirement R2 ".....to ensure that personnel maintain awareness of the cyber security practices that are essential to protecting BES Cyber Systems." Consider whether it is necessary to state the justification for each Requirement, especially if it could be that the objectives achieved by the Requirement are not exactly as specified or if the Requirement does not necessarily meet the objective as set out. It would be preferable to just have the broad purpose statement in the introduction which is stated to apply to each of the Requirements that follow. What is the purpose of the Measures in these standards? If they are to re-state the wording of the Requirement, they provide no value and create opportunities for legal interpretation if the wording in the measure does not exactly match the wording in the specific requirement. Entities should be allowed to employ multiple layers and tailor their approaches to cyber security to meet the intent of the requirement, such as including the inherent security benefits provided by private entity owned and managed communication networks. Manitoba Hydro is also concerned that the multiple layers of physical and electronic security directed by FERC Order 706 are

#	Organization	Question 54 Comment
		not included in this proposed version of the CIP-010 and CIP-011. While we understand that these directives were not included at this time for the sake of expediency, there is a risk that the electric industry may expend considerable resources to meet the requirements these proposed standards, only to revisit the electronic and physical security issues and expend more resources in the near future. Implementing physical security changes for electric facilities is proving to be a monumental task. This standard does a disservice to the industry if it does not provide the complete scope of the physical security changes required. If the entire scope of the physical security requirements, including the directives in FERC Order 706, cannot be provided to the industry in this proposed version of the standard, then all the requirements for physical security should be removed at this time and submitted to the industry, in its entirety, at a later date.
54.42	Alberta Electric System Operator	Specifying the units of measure (e.g. business vs. calendar days) and exact ordinal amounts ("365 days from date of implementation" vs. "annually") might help resolve some ambiguity surrounding some of the criteria.
54.43	Northeast Power Coordinating Council	Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional page.Request that the tables and time constraints be consistent. Also where the document refers to processes in some cases it specifies one or more processes and in others just processes. Eliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (refer to R5-R32).Request a cross-reference of CIP-011 Requirements that refers to another CIP-011 Requirement, with emphasis on the Access Control Requirements. A diagram might help.Remove adjectives such as substantial, adequate, minimum, etc., as these are difficult to measure and can lead to different interpretations.Situational awareness displays currently in use at the Regions and FERC should not be included in the applicability of these standards. No operational actions or decisions are being made based on the information on those displays.
54.44	Nuclear Energy Institute	Terms should be clearly defined and unambiguous. Examples of items covered by the term and not covered by the term should be given. CIP-011-1 is a vast change from the prior CIP-003 through CIP-009, and clear definitions with examples will be valuable.

#	Organization	Question 54 Comment
54.45	Puget Sound Energy	The amount of work relative to CIP-010 is almost as much as CIP-010 because of the broad application of BES Cyber Systems. It would be prefereable to be able to manage this scope better up front so that entities don't have to evaluate and record so much to then only focus possibly a much smaller pool of work as more defined by CIP-011. It still not clear how to evaluate a system for "misuse" effectively and defensibly. Further guidance would be appreciated. Lastly their should be some grace period and easier interpretation process when these versions become effective in order to more quickly flush out interpretations of concepts once implementation starts. To date the interpretation is a lengthy process or determined in an audit as a result of a violation when the entity may have been well intended.
54.46	APPA Task Force	The APPA Task Force commends the drafting team on the overall development of CIP-011-1. We believe this document is another step in the right direction of cyber system protection. We did, however, notice a theme throughout the requirements that caused us some concern. There is an IT focus to a number of the requirements. The drafting team seemed to be focusing on control centers when developing requirements to protect critical facilities. As a result, a number of the requirements are not practical for remote substations and generation stations, that may be owned by many entities and operated by only one of them, or another entity. What may be simple in a control center environment may be next to impossible for a transmission substation or a generator.
54.47	Constellation Energy Commodities Group Inc.	The blank boxes in CIP-011 tables need to be filled in. While the intent appears to be that if the box is blank the control is not required, by leaving it blank, liability questions could be raised. Compensatory measures should be allowed in the compliance structure. Entities may find that alternative, but comparable protection measures will better fit the circumstances of their system.An audit standardization or guidance document should be developed for use by auditors/reviewers of compliance to NERC CIP standards. Even though the formalization of cyber protection compliance programs are relatively new within the NERC standards body, there are mature examples of cyber protection and information security controls frameworks comprised of formalized cyber security standards, compliance management methodologies and auditing guidance such as defined in NIST 800-XX and ISO 2700X regimens . These regimens include guidance and standardization for auditing compliance (e.g., NIST SP800-53A). Other examples of formalized auditing guidance include guidance

#	Organization	Question 54 Comment
		documents published by ISACA (Information System Audit and Control Association). These regimens include formal auditing guidance to ensure comprehensive coverage of compliance requirements, consistency in auditing approaches and better insight for being audited in ensuring auditability for their compliance audits. This improves the effectiveness as well as the business efficiency of companies' compliance programs. This rationale also applies to the NERC CIP program.The Implementation Plan should allow for sufficient time to complete the comprehensive task of identifying and categorizing BES cyber systems.The R3 and R4 tables should address each requirement. All tables should be completed in full stating either not applicable or required.
54.48	Midwest ISO	The categorization approach in CIP-010 appears to require any BES Cyber System that touches the BES in any way to be included no matter how minimal the impact of the Cyber System on the BES, we are concerned that the Midwest ISO energy and ancillary services markets will be impacted. We believe that market portals could become High, Medium or Low Impact facilities and, thus, require application of the CIP standards or modification of the systems to isolate them so that CIP standards don't apply. Our conservative estimate is that we could easily spend in excess of $10 million dollars without anywhere close to this impact because our existing processes would prevent the market from negatively impacting reliability. We request that the drafting team make clear that market systems should not be included per NERC standard development tenets. In some cases, drawing in market systems could present impossible challenges. For instance, if a market portal becomes a High Impact BES Cyber System, CIP-011 R4 appears to require that we would have to conduct personnel risk assessments on all users which would include thousands of employees from market participants submitting bids and offers. State laws make this impossible. The drafting team could help solve this problem by making clear that personnel does not include market participants/customers who already have significant financial incentive to enter good bid and offer data. Opportunity costs do not appear to be considered in the development of these standards. All business resources are limited. Requiring registered entities to focus on these specific issues may divert attention away from other important cyber and physical security initiatives and work that offer greater improvements to reliability.We are also concerned that cyber and physical security could initially be compromised as entities focus on becoming compliant for Low and Medium impact cyber systems. Likely, High Impact Cyber systems will meet the new requirements because they were likely Critical Cyber Assets under the existing CIP standards. Thus, their reliability could degrade as entities may lose focus on the High Impact BES

#	Organization	Question 54 Comment
		Cyber Systems.
54.49	Florida Municipal Power Agency	The drafting team seems to have added an objective into the requirements which adds ambiguity to the requirement. For instance, R2 adds the phrase “to ensure that personnel maintain awareness ...” which adds ambiguity to the requirement. Is the auditor going to measure “quarterly reinforcement” or “personnel ... awareness” or both? If the drafting team wishes to add an objective to each of the requirements, then consider one of two other alternatives: (1) adopt International Standards Organization format where they have an objective for each requirement introducing each requirement; or (2) develop a longer Purpose section where the purpose of each of the requirements is further embellished.Throughout the standard, there is confusion among the terms “grant” and “authorize”. “Authorize” is senior manager approval, “grant” is giving the person a key, keycard, or user account. The requirements should keep these two concepts clear. For instance, in 5.5, “authorize” should be changed to something like: “Grant unescorted physical access to areas containing BES Cyber Systems only to those who are authorized such access”.Overall, added complexity to the cyber systems will reduce the reliability of the BES, so this needs to be kept in mind when drafting these standards.Almost all of the standards need to have stronger language in them to remove ambiguity and give specific guidelines as to what it expected.
54.50	NextEra Energy Corporate Compliance	The following are specific language changes for clarity:1. Title: Cyber Security - BES Cyber System Protection 2. Number: CIP-011-1 3. Purpose: To provide clear understanding of the protections that are to be applied to BES Cyber System Components identified as a result of the applicable of CIP-010-1 to the Responsible Entity’s BES.Also, for clarity, this section should be re-written as follows:R2. Each Responsible Entity shall reinforce sound security practices to all employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access to a BES Cyber System Component reinforcements in sound security practices at the beginning of each quarter. The Responsible Entity also has the discretion to reinforce sound security practices at any time, it deems appropriate. The reinforcement may be delivered via e-mail, intranet, posters, classes or other educations methods. .R3. Prior to granting employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access, each Responsible Entity shall ensure the personnel requesting access completes cyber security training consistent with that required in. CIP-011-1 Table R3 - Cyber Security Training,.3.1. For employees and contractor personnel requesting

#	Organization	Question 54 Comment
		authorized cyber access, this cyber security training shall cover the following: o The proper use of BES Cyber Systems o Physical access controls to BES Cyber Systems o Visitor control program o The proper handling of BES Cyber Systems information and storage media o Identification and reporting of a Cyber Security Incident For employees and contractor personnel requesting only unescorted physical access, this cyber security training shall cover the following: Procedures for not intervening with a BES Cyber System ComponentVisitor control programIdentification and reporting of a Cyber Security Incident 3.2. For employees and contractors personnel who engage in the operation or control of the BES via authorized cyber access to a BES Cyber System Component, cyber security training shall additionally include training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber System Components and BES Cyber Systems. 3.3. For employees and contractor personnel who have a role in BES Cyber System recovery this cyber security training shall additionally include those related action plans and procedures to recover or re-establish BES Cyber Systems. For employee and contractor personnel who have a role in BES Cyber System incident response this cyber security training shall additionally include those related action plans and procedures.3.4. For employee and contractor personnel who have a role in BES Cyber System incident response this cyber security training shall additionally include those related action plans and procedures. 3.5. Each Responsible Entity shall maintain document for each employee and contractor personnel required to take cyber security training as required in R3 and its sub-requirements that the training was conducted at least once every 12 months plus or minus one month. R4. Prior to granting employee and contractor personnel who have authorized cyber access and/or authorized unescorted physical access, each Responsible Entity shall perform or have performed a personnel risk assessment on the employee or contractor personnel requesting access consistent with CIP-011-1 Table R4 - Personnel Risk Assessment, expect as prohibited or limited by federal, state, provincial, and local laws, and existing collective bargaining unit agreements. 4.1. This personnel risk assessment program shall at a minimum include: o Identity verification via photographic identification documentation issued by a government agency (i.e., Federal, State or Provincial); and o A seven year criminal history screened against specific criteria developed and documented by the Responsible Entity. The seven year criminal history shall include a records check that covers all locations where, during the previous seven years up to date the check was performed, the subject has resided, been employed, and/or attended school for six months or more, including

#	Organization	Question 54 Comment
		current residence regardless of duration. 4.2. Each Responsible Entity shall document the results of each personnel risk assessment. 4.3. Each Responsible Entity shall update or have updated each personnel risk assessment at least once every seven years after the initial personnel risk assessment.
54.51	Entergy	The industry has now had experience grappling with a one-size-fits-all set of cyber security standards' requirements for its grid and generation control systems. At a high level of abstraction the problems with this approach are manifest in two major ways. The first concerns the age of the control system components we have at work relative to cyber vulnerabilities, threats, and hence risk. In brief, our control host systems and operator consoles by and large today use mainstream "IT" commercial off the shelf computer (COTS) hardware, operating systems, and application code bases. These are the very same networked-computing systems components that are widely hacked on the Internet and within mainstream commercial businesses around the world, and accordingly represent highest risk to reliable grid operation from cyber malfunction or nefarious attack. If hacked, they provide the ability for perpetrators to commandeer and use the systems against us - which represents the worst case scenario (e.g., a widespread unplanned "load shedding event" - trip all). On the other far extreme, we have often decades-old computing equipment still widely used "in the field" at substations, switching stations, hydro dams, etc. Increasingly these field sites are connected to control hosts over ("Internet") routable protocol communications networks, and increasingly emergent wireless communications transmission technologies. But there also remains very high dependency on "legacy serial" and "POTS" dial-up communications. So, we have both very old and very new networked-computing control systems technology woven together that requires some kind of cyber security protection. The second major distinction is the physical orientation of control host and generating plant sites on the one hand, and the far flung field assets on the other. The former are typically referred to in security circles as "bastion sites," in that they can be defended in much the same way as castles of old using concentric rings of physical defenses, complimented by armed guards. The field sites on the other hand have more in common with gas and oil pipelines, rail infrastructure, and the like that are characterized by long stretches of geographical separation between sites. These are hard to physically defend economically, and, through use of protocols that by design enable "network navigation" akin to being able to telephone-dial anyone in the country on demand, provide an attack vector path back to control hosts, and therewith also creating opportunities for "island hoping" from one organizational network to another. Given these two decidedly different continuums of variables that the industry needs to

#	Organization	Question 54 Comment
		defend, “one size fits all” standards’ requirements result in situations where the requirements are expensive overkill in one circumstance, and if watered-down to ease this burden do not provide robust enough protections for the circumstance at the other end of the spectrum. The only standards-writing approach that affords appropriate cost-effective security is to define granular sets of standards that are specific to the real vulnerabilities and threats incumbent to each scenario. From this perspective, specific recommendations for improving the current Version 4 draft CIP Standards are outlined below.The SDT was directed in Order 706 to consider adaptation of the NIST Security Risk Management Framework, especially noting SP800-53. This comment is neither about the individual requirements themselves nor the fact that most of the specific CIP-011-1 requirement language was drawn from the DHS Catalog of Controls. Rather, this comment focuses on the fact that the SDT has diverged from FERC directive in not employing a major foundational construct of SP800-53. Specifically, the SDT has developed a single set of requirements, and then through use of sub-requirement tables indicate in binary fashion whether or not each (sub)requirement of note is applicable or not, based strictly on the high-medium-low “impact categorization” based exclusively upon a facility’s size (electrical operating characteristics). Contrast this with the SP800-53 paradigm, where there are three graduated, hierarchical layers of cyber security control and countermeasure requirements. First, there is a baseline set of requirements, which applies for all cyber systems, and these are the only requirements applicable for low-impact-on-mission cyber systems. Then, there is a second and third set of requirements that apply cumulatively for medium and high mission-impact cyber systems respectively. The SP800-53 approach is responsive to the stated FERC preference that there be a baseline set of requirements that must apply for all grid BES Cyber Systems/Components. Draft CIP-010-1 is not responsive to FERC Order 706 - many requirements as stated in the Standards’ language simply do not apply for BES Cyber Systems/Components in use at low and medium-sized grid sites.Recommendation: A) Modify the categorization of grid assets (Attachment II) into two groups:i) “Bastion Installations” consisting of data centers, control centers, and generation sites. Rationale: At least the ‘data center’ part tends to employ mainstream IT COTS HW/OS/and to some degree appl code; and, physical security measures can be used to greater advantage as compensating measures where cyber security measures may be difficult to implement for a variety of reasonsii) “Grid Field Assets” consisting of any physical site that does not have a control host/control center within their physical perimeters, regardless of what protocols are in use. The distinction again revolves around

#	Organization	Question 54 Comment
		physical security, in this case the difficulty in physically securing far flung field sites.B) Create layers of requirements akin to the SP800-53 paradigm, labeled 'a-z': i) The lowest enumerations being baseline requirements; e.g., 'a' could be associated with bastion installations, and 'b' could pertain for field grid asset sites. Important distinctions at the baseline can pertain for each site type.ii) Similarly, create appropriate sets of succeeding requirements applicable specifically to each column (bastion/field) depending on the type of data networking communications employed. This way appropriate requirements - not more nor less than necessary - and be specified for the unique characteristics and attack surfaces posed by each technology. As technologies are retired, e.g., serial legacy, POTS dial-up, so can entire categories of requirements.C) Create a "Scoping Table" consisting of: i) Two columns: Bastion/Field - #1 above); and,ii) X number of rows: #2 above - list of different communications technologies, i.e., routed, legacy serial, dial-up, non-routed LAN, non-routed wireless, etc., as the SDT deems appropriate. D) Apply requirements sets (a-z) as appropriate within each box on the grid.2) Entergy submits that NERC's intention to address the following FERC Order 706 directives in action subsequent to adoption of CIP Version 4 will create undue hardship for the industry. The following Order 706 directives are central to implementation of any organizational cyber security program, and it is unreasonable, inefficient, and potentially financially wasteful to require the industry to implement one approach per Version 4 Requirements, and then be made to re-visit entire cyber security programs in order to comply with post Version 4 changes. Entergy submits that the entire puzzle should be addressed at once, i.e., including the following FERC Order 706 directives, at the same time while recasting the CIP Standards under Version 4:...develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter... a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.... consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.... revise the Reliability Standard to require two or more defensive measures.... modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years... that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a

#	Organization	Question 54 Comment
		physical security perimeter around critical cyber assets.... consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.... provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.... to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.... to revise CIP-009-1 to require data collection, as provided in the Blackout Report.... proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.Entergy recommends that NERC appeal to FERC for permission to extend the deadline for final Version 4 drafting a modest amount of time necessary for the entire puzzle to be grappled at once. The industry is now hardly complete in implementation of CIP V1-V3 Standards' Requirements. The prospect of having to endure adaptation to two more waves of fundamental change to the tenets of these standards is not only onerous, but also not responsive to the imperative to provide service at lowest reasonable cost to ratepayers. We didn't build our national electric infrastructure overnight, and apt response to relatively recent emergence of cyber security threats will not be accomplished overnight either.
54.52	IRC Standards Review Committee	The organization of the 32 requirements and all of the subrequirements is lesser of a concern to us, although separate standards that group similar requirements allows for better administration. The greater concern is the degree of specificity of many of these standards. As discussed in the response to Q #8, many of these requirements go into exacting detail specific to technology and may duplicate either other industry standards or practices already employed. Many of these requirements can be elevated to "higher level" requirements that requires certain types of protections, e.g. - require user access identification, rather than specific password practices. For examples, the list of criteria that are included in Requirements Table R9, the details in the Tables for R10 and R11, and the specific treatment of wireless access in R12, to name a few.
54.53	Public Service Enterprise	The requirements for wireless and remote access (R11 to R14) are not well integrated with other

#	Organization	Question 54 Comment
	Group companies	requirements for access to BES Cyber Security Systems (R7 to R10).
54.54	PNGC-Cowtitz-Central Lincoln-Benton-Clallam Group	The table format is great, makes it very easy to see what applies.If we say “CIP-011-1 R3.1” do you know what we am referring to? There is a sub-requirement 3.1 as well as a line 3.1 in Table R3. This could lead to confusion. Suggest extending the table to cover all sub-requirements, or otherwise avoid repeating numbers. This occurs only in R3 and R4.Regarding R21, no definitions have been provided for “other cyber systems” and “Cyber System Components” (without “BES” in the phrase.) Note that “Cyber System Components” is capitalized as if it was defined, but no definition exists or is proposed. While “other cyber systems” is not capitalized, it should also be defined to avoid any ambiguity over what the SDT intends. We appreciate the objectives that the SDT has included in the requirements, since this will help us to see the SDT’s intent. There is the risk, however, that auditors will see this as more than guidance when placed in the requirement. For example, an auditor might read R5 and R6 as requiring the prevention and/or detection of all unauthorized physical access, and find an entity non-compliant for an undetected or un-prevented intrusion. We suggest the objectives (“to prevent..”, “to ensure..”, etc.) be placed in the guidance document, or otherwise be removed from the requirements. Note that some of these objectives when read as requirements are absolute, such as R14; “..to ensure no unauthorized access is allowed.
54.55	MidAmerican Energy Company	The term "Annual" is not defined. Define "Annual" in the NERC glossary to be 12 months not to exceed 15 months. Change all 12 month references back to "Annual".The following provides a summary of the reasons for using a definition of “12 months not to exceed 15 months.” o It does not force “creep.” A definition of 365 days or 12 months, without a “not to exceed” clause means that work must be planned to be done enough before the 365 days to allow time for unexpected situations. This can result in doing “annual” requirements every 10 months or less to ensure compliance is not jeopardized. o It does not jeopardize compliance for either delivery or supply due to current implementation plans. A calendar year definition could unintentionally jeopardize compliance if delivery did not complete a task between June 30 and Dec. 31, 2009. o There is no effect of leap years, which could be a problem with a definition of 365 days._____Requirements that are defined to be completed within x hours are impractical and unnecessary. Entities do not currently document the precise hour that (as an example) a termination takes place. Thus hourly requirements are impractical to measure or audit.

#	Organization	Question 54 Comment
		Convert all hourly requirement as follows: o Convert 1 Hour requirements to "As soon as possible not to exceed date reported". o Convert 4 Hour requirements to "As soon as possible not to exceed date reported". o Convert 6 Hour requirements to "As soon as possible not to exceed date reported". o Convert 12 Hour requirements to "As soon as possible not to exceed date reported". o Convert 24 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 36 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 48 Hour requirements to "As soon as possible not to exceed next day from date reported". o Convert 72 Hour requirements to "As soon as possible not to exceed second day from date reported"._____The following FERC Directives need to be addressed with version 1 of CIP-010 and CIP-011: o 2 or more diverse security measures for defense in depth at the security boundaries o Active vulnerability assessments every 3 years o Incorporate forensic data collection and proceduresThe framework is in place to incorporate requirements in CIP-011 that address the directives. CIP-011 has a potentially long implementation time. FERC will likely not wait for the implementation of CIP-011-1 to be complete prior to making NERC address these directives. Incorporating these directives in the middle of the implementation of CIP-011-1 will be confusing and cause additional expense and effort. Entities will be required to make additional expenditures at greater cost if these issues are resolved in later versions. NERC should ask FERC for more time to implement version 1 if necessary.
54.56	Dairyland Power Cooperative	There are very few requirements that apply to low impact systems and many that do not apply to medium impact systems. Considering that many high impact systems will connect with lower impact systems, how will data integrity be adequately implemented? Consider a large RTO/ISO connecting a shared communications system to all entities in a region, regardless of impact to the BES.The standard basically excludes serial communications from being governed. This not only does not address protecting serial systems, but it introduces oddities and ambiguities about routable connections in relation to serial connections. There are security questions, as well as questions as to how such connections will be viewed by an auditor. Serial communications should not be ignored.
54.57	Ameren	These standards will require a substantional amount of effort to implement for entities while also maintianing compliance with the previous versions of the CIP standards, how will the implementation schedule address this? Will their be a period were the entity does not have to comply with the old

#	Organization	Question 54 Comment
		standards while implementing the new standards, for examle 30 days to 90 days while the entity is updating systems or updating/revising procedures for the new standards. Also, the local definitions should be included in the NERC glossary of terms rather than by the standard to which they apply.
54.58	Bonneville Power Administration	This is far better than the current standards. The requirements are more straight forward by not cross referencing each other in separate standards. Much time is spent "mapping" out how the standards relate to each other and under what specific requirements. If misinterpreted it could lead to potential violations. This is a much better approach. Not directly relating to the newly proposed standards but still a concern is the time for implementation. Numerous resources have been extended and significant dollars spent to meet the current requirements. There needs to be sufficient time to review the new standards, identify Cyber Systems and allow for proper prior planning to physically protect these systems. Depending on the category, low-high, significantly more dollars could be spent. There needs to be sufficient time to address the new standards and implement in a manner that is cost effective. The overall approach is superb: target the standards only at systems that can actually affect the BES in near-real time, include other systems only to the minimum extent necessary, require outcomes rather than specify actions. However, this draft has some wording issues that apparently have inadvertently broadened the scope far beyond the intent of the SDT, or even practicality. As described above, correcting these errors will produce a set of standards that enforce security where it needs to be, but do not waste time, money, and people addressing tasks that do not improve the security of the BES. In particular, we find that the following questions address issues that must be corrected before the standards could be acceptable:- Q5, addressing CIP-010 Table R3 Section 3.2- Q12, addressing CIP-011 Table R3 Section 3.2- Q13, addressing the the definition of "External Connectivity". Note that several other questions rely upon changing this definition.- Q16, addressing CIP-011 Table R5, sections 5.8 and 5.9- Q22 and Q23, addressing revocation time limits- Q24, addressing authentication schemes- Q27, definition of "Remote Access"- Q32, addressing revocation of remote access- Q33, addressing Table R14 Sections 13.2 and 14.4- Q35, addressing Table R16, Section 16.2 and patch risk assessment- Q35, addressing Table R17, Section 17.2 and disabling of physical ports- Q35, addressing Table R18, Sections 18.1, 18.2, 18.3, and 18.4- Q37, addressing Table R20, Sections 20.1, 20.2, 20.3, 20.6- Q37, addressing Table R21, Section 21.1- Q38, addressing the second part of the definition of electronic access point. This is the most serious flaw in the standard. It must be corrected.- Q40, addressing Table R23 section 23.7- Q42, addressing the definition of

#	Organization	Question 54 Comment
		sensitive information- Q44, addressing Table R24, Section 24.1 and 24.3- Q47, addressing Table R26, section 26.2- Q51, addressing Table R30, Section 30.5- Q51, addressing Table R31, sections 31.1 and 31.2- Q53, addressing TFEs Overall, an excellent start. Here are some additional suggestions:1. In all cases - Write the standards to identify the outcome of the requirement. Never say how to do something, say what you intend for it to accomplish. Let the Responsible Entities figure out the "how".2. Use Industry Standard wording wherever possible. For example, the term "Hardened" means one thing in IT and another in a substation.3. Define any terms that may present confusion - Example - Ports and services. There is a common IT understanding when you hear that term. It is almost always assumed to mean logical ports 0 to 65535 and the networking services they support. However, it can also mean physical ports like Ethernet jacks, RJ45, Serial connectors, parallel connections etc. If there is a question, put it in the definitions.4. Wherever possible, include all the elements of a standard into one standard. Only break requirements apart where it makes real sense to do so. So If you get to R32 and find that something there seems to fit in 20, go back and put it there rather than making a reference back. 5. Keep paring this down in size. It is so much better.6. If any of your experts know that equipment used in the electrical generation and distribution industry cannot perform specific functions, don't write the standards to say they have to.7. There were questions in the May webinar about the meaning of "revocation". Our suggestion is this: revocation is the act of ensuring that a person can no longer gain access to a system, physical area, or information. It can be accomplished directly or indirectly. For instance, if a cyber asset is only accessible from within a physical facility, then denying physical access to the facility also denies cyber access to the cyber asset. If sensitive information on a system resides only in electronic form on particular servers, then denying cyber access to those servers denies access to the information. The emphasis should be on the denial of access, not how that denial is accomplished.Definition of "annual" or "annually": There are numerous occurrences of these terms in the Requirements. Also now, Requirements state that activities must occur “at least once every 12, 24, or 36 months.” Similar to the comment on R1, the SDT should ensure that the highlighted language says exactly what it means. “/A/t least once every 12 months” could lead to some confusion. Let’s assume that the event occurred on July 15, 2010, and again on March 15, 2011. That is “at least once every 12 months.” But it raises the question of when the next activity or compliance event must occur. Is it no later than July 15, 2011, or no later than March 15, 2012? The exact questions could be asked for events that are supposed to occur “at

#	Organization	Question 54 Comment
		least once every 24 or 36 months."Following on to comment 1 immediately above, there are two other phrases that could be used depending on what NERC intends. o "every 12 months" - in this case, the event would occur on the same date each year. This would be virtually impossible. Same concern with "every 24 or 36 months." o "within 12 months of" the event - in this case let's assume that the event occurred on March 15, 2010. The next event would have to occur no later than March 15, 2011, but could occur earlier (let's say it occurred on December 15, 2010). If it occurred on December 15, 2010, the next event would have to occur no later than December 15, 2011. The same example with different dates would work for "at least once every 24 or 36 months."The SDT should be very specific as to what it means for how frequently the events referenced above must occur. BPA appreciates the opportunity to provide comments. Thank you.
54.59	MRO's NERC Standards Review Subcommittee	We believe all of the requirements that specify something to be completed within X hours would be better suited to the following language: "As soon as practical, but not to exceed x business days from the date reported". This would maintain the spirit of the requirement, while also allowing for more practical time frames.With so many auditable elements included within the requirements, we believe the VSL's cannot be written with the current zero-defect mentality. We feel a practical approach is required, where minor issues are allowed to be addressed without representing immediate non-compliance and associated investigations and settlement proceedings, but instead are identified and scheduled for corrective action.We understand the burden on the drafting team to meet FERC's deadlines, but we would propose that all outstanding FERC directives be addressed as part of the current process, as opposed to leaving some items for a later date.
54.60	Idaho Power Company	We commend the SDT on its efforts to draft a standard that meets the FERC directives but is feasible for the industry to implement. That is an extremely difficult assignment. This version will greatly expand the number of cyber assets that are impacted by the CIP requirements and represents a major shift in the identification and classification of an entities BES cyber systems. We are certainly willing to implement the standards because we understand the impact of failure to do so. However, the standards must be accompanied by as much guidance documentation as possible along with realistic implementation plans that take into account the technology required, time required to realistically implement the controls, the fact that registered entities must first assess the financial impact and then

#	Organization	Question 54 Comment
		budget appropriately, and the massive volume of work that implementation represents.
54.61	Xcel Energy	We do not agree that Low impact systems should have mandatory, enforceable cyber security standards. By their very definition, Low impact systems have very little potential to impact the BES. As such, cyber security controls on these systems is best left to the business judgment of each individual entity. The terms defined throughout the standard have not followed the convention of being capitalized. They should be capitalized so that it is clear to the reader that they are defined terms when they are used later in the standard. The Standard would be enhanced if it were to differentiate between software based versus firmware based devices.The Standard would also be enhanced if it were to separately define requirements for Control Centers, Substations, and Generation Facilities. The cyber security issues between these different types of facilities are vastly different. Transmission Control Centers are typically fully digital control systems with the ability to have wide area impacts. On the other extreme, where Generation facilities typically have digital systems are for retrofits to older, analog systems controlling individual components within the facility, such as digital feedwater or digital turbine controls. These are much different that Transmission Control Centers as they have only limited, local impact. Additionally, they typically have mechanical controls that can override the digital systems providing limited, if any benefit from protecting the digital aspects of the system from malicious attacks.
54.62	We Energies	We Energies agrees with EEI: Please see the earlier discussion about identification of a rational and understandable threat basis that should be used when constructing security requirements. The requirements should focus on the highest probability risks that will have the most negative impact. The requirements should not treat all threats and impacts equally.
54.63	Duke Energy	We had previously gone a long way towards getting common understanding on terms such as “Critical Assets”, Critical Cyber Assets”, “Electronic Security Perimeter” and Physical Security Perimeter”. Moving away from these terms in the current Version 4 draft creates uncertainty.Tables and subrequirements should have different numbering schemes so that, for example, there are not two 3.1 listings.If the standard is broken into smaller standards, please provide separate measures for each standard.

#	Organization	Question 54 Comment
54.64	Hydro One	We noticed that combined CIP-011-4 standard excluded vulnerability management program. We'd like to know what the rationale was behind this decision and if this might be considered in the next draft.Suggestion for an additional page that repeats all of the local definitions - this means the local definitions exist in the document as is plus this additional page.Request that the tables and time constraints be consistent. Also where the document refers to processes in some cases it specifies one or more processes and in others just processes. Eliminate confusion caused by two 3.1's. Some Requirements list sub-requirements. Most Requirements use tables for sub-Requirements (refer to R5-R32).Request a cross-reference of CIP-011 Requirements that refers to another CIP-011 Requirement, with emphasis on the Access Control Requirements. A diagram might help.Remove adjectives such as substantial, adequate, minimum, etc., as these are difficult to measure and can lead to different interpretations.
54.65	GTC & GSOC	We recommend a local definition of "Implement" should be added to CIP 011: "Implement means to put into place and consistently utilize. An entity has implemented a policy, procedure, or plan when it has created such policy, procedure or plan and consistently uses it in appropriate circumstances."Throughout the standards the inclusion of the words "for external connectivity only" in the tables is redundant and confusing. If used at all, the qualifier should be on "access" in the text of the standard rather than in the table.We recommend Annual be defined as recurring at least once every Calendar year and at least once within any thirteen (13) consecutive calendar months. Otherwise, annual training will necessarily have to take place earlier each calendar year to ensure all personnel are trained within twelve (12) months.We appreciate the significant effort that the NERC Cyber Security Order 706 Standards Drafting Team has put into developing these proposed standards and communicating them to the industry, especially the CIP Workshop held in Grapevine, TX. We are in full support of the NERC standards development process for the development of reliability standards to secure and protect North America's critical electric infrastructure. In particular, we appreciate the multiple opportunities to guide the development of the CIP standards through both informal and formal comment periods. We are supportive of the proposed standards. We believe these standards are a significant step forward in terms of being able to clearly understand the expectations that are placed upon the entity as well as the security that they provide for the Bulk Electric System.

#	Organization	Question 54 Comment
54.66	PNM Resources, Inc.	We suggest not removing explicit examples from the language of the standards. The incorporation of examples provides clarity and brightline guidance that improves a Responsible Entity's opportunity to comply with the standard. The introduction of new and additional "flexibility" can lead to ambiguity and differences of opinion between the entities and auditors and creatr more opportunities for Regional Entities to allege violations.
54.67	MWDSC	When looking at logical tasks to mitigate risk, e.g., malicious code propagation, could a malicious code in one cyber component affect another component and result in a change in the impact categorization, e.g., low vs medium?
54.68	Progress Energy - Nuclear Generation	Yes, see comments a - f below.a. Comments: Attachment 1 included in responses above follows this question. To obtain full benefit of this review, see Attachment 1.b. The security controls in CIP-011-1 should provide for acceptance of Common Controls as defined by NIST 800-53. CIP-011-1 would offer a more consistent approach in cyber security regulation by considering the mature physical security programs, engineering control programs, emergency plans and physical segregation programs within the nuclear industry that offer alternative countermeasures. These countermeasures provide at least the same degree of cyber security protection as the corresponding cyber security control. c. NIST 800-53 establishes provision for tailoring security controls and states that the level of detail required in documenting tailoring decisions in the security control selection process is strictly at the discretion of the organization consistent with the impact level of the information system. CIP-010-1 and CIP-011-1 should allow use of this provision in the nuclear industry consistent with acceptance by nuclear regulators.d. Nuclear applicability is specified in CIP-010-1, Section 4.2.1. The following comments are based on applicability to nuclear generating facilities: o Definitions for Bulk Electrical System (BES) Cyber System and BES Cyber System Component conflict with definitions that have been accepted by the NRC in NEI 08-09, Revision 6, for Critical System and Critical Digital Asset. Recommend, that for nuclear systems subject to FERC Order 706-B, that definitions for FERC and NRC regulated systems be consistent. o CIP-010-1 requirement R2 and Attachment 1 - some of these functions are covered by NRC regulation. Will issuance of this document require re-submittal of systems for exemption after the Bright Line submittal of systems? o The implementation schedule for CIP-010-1 and CIP-011-1 versus CIPs 002 through 009 requires doing the same reviews twice and is an unnecessary burden on

#	Organization	Question 54 Comment
		nuclear licensees as well as other FERC critical assets.e. Several requirements include periodic review of controls (e.g., R8.2, R12.1). This CIP should contain a provision that permits nuclear facilities to use the periodicities in its NRC approved Cyber Security Program in lieu of those in the CIP standards. This allowance would minimize the administrative burden of having two sets of requirements for the same Cyber Security programmatic element so that plant digital systems that support safety, security, EP or BOP functions are not regulated differently. The following are used to establish frequency or periodicity for security controls with identified durations: o NRC Regulations, Orders o Operating License Requirements (e.g., Technical Specifications) o Site operating history o Industry operating experience o Experience with security control o Guidance in generally accepted standards (e.g., NIST, IEEE, ISO) o Audits and Assessments o Benchmarking o Availability of new technologies. f. R27.1 - The definition of "Cyber Security Incident" should be revisited in light of current definitions, especially NRC and NEI, and revised to align with the definition of "Cyber Attack." It is not on the list of terms to be defined. From NERC Glossary of Terms used in NERC Reliability Standards updated April 20, 2010, the "Cyber Security Incident" definition is: o Any malicious act or suspicious event that:o Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,o Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.o It is unclear what NERC does with cyber incident reports and whether these reports are consistent with those required by the NRC in the event of a "cyber attack." Progress Energy Nuclear Generation Group CommentsCIP- 011-1ATTACHMENT 1NIST Security Control Description NIST 800-53 NEI 08-09 NEI 08-09 Description CIP-011-1 CIP-011 Description NRC CommentsSecurity Planning Policy and Procedures PL-1 N/A N/A R1 Security Governance and Policy 50 App B 50 App E73.5473.5573.56 The development and implementation of cyber security policies that address the requirements identified in R1 are mandated for nuclear by one or more Code of Federal Regulations (CFR). This requirement duplicates and/or is not consistent with the CFR and could lead to regulatory uncertainty. Review of cyber security is mandated by 73.55(m) and R1 conflicts with its duration. This would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant.Security Awareness AT-2 E9.2 Awareness Training R2 Personnel Training, Awareness and Risk Assessment 73.5450 App B Training requirements for nuclear personnel are established by CFR. R 3.3.2 would result in personnel without a need to know becoming knowledgeable in technical aspects of digital equipment. R3.3.4 is not required for users to perform

#	Organization	Question 54 Comment
		their job. This conflicts with 73.54 requirements that personnel are trained to the extent necessary to perform their assigned duties. This would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant.Security Training AT-3 N/A N/A R3 Personnel Training, Awareness and Risk Assessment 73.5473.55 Physical and logical access to plant digital systems is governed by CFR. Personnel who are granted access to these systems are required to complete training that result in their receiving formal and documented Qualifications. Requalification is at established intervals required by plant procedures. Whether the plant system performs functions associated with safety, security, emergency preparedness or BOP, the requirements are the same. Additional training and duration not consistent with established mature training programs would result in conflicting requirements for BOP systems and would result in dual regulation for the nuclear plant. R4 Personnel Risk Assessment 73.56 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. Results are documented and stored in Records. The requirements in R4 conflict with the requirements in the CFR that nuclear personnel supporting plant system performs functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from requirement R4. R5.1 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted unescorted physical access to nuclear plants. The nuclear plant is protected by armed security officers and other protective strategy that restricts access. The requirements in R5.1-3 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.2 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.2 are covered by the CFR for restricting physical access for all plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.3 Physical Security for BES Cyber

#	Organization	Question 54 Comment
		Systems 73.55 Nuclear personnel must pass through security access points before being granted physical access to nuclear plants. Automated scanning records entry. The requirements in R5.3 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Monitoring Physical Access PE-6 E5.8 Monitoring Physical Access R5.4 Physical Security for BES Cyber Systems 73.55 Visitors must receive approval prior to arriving at the security access points and are subject to search before being granted physical access to nuclear plants. Entry and exit are documented. The requirements in R5.4 are covered by the CFR for nuclear visitors supporting plant systems performing functions associated with safety, security, emergency preparedness, BOP or other. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Physical Access Authorizations PE-2 E5.4 Physical Access Authorizations R5.5 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. before being granted unescorted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.5 are covered by the CFR for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement.Physical Access Control PE-3 E5.5 Physical Access Control R5.6 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are subject to annual retraining in order to maintain unescorted physical access to nuclear plants. Results are documented and stored in Records. The requirements in R5.6 conflict with the CFR that cover access authorization for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently. Consider exempting nuclear facilities from this requirement. R5.7 Physical Security for BES Cyber Systems Part 2673.56 Requirements for nuclear personnel terminated for cause are covered by the CFR. The requirements in R5.7 conflict with the CFR that direct termination for cause of nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting

#	Organization	Question 54 Comment
		nuclear facilities from this requirement. R5.8 Physical Security for BES Cyber Systems 73.55 N/A to nuclear - applicable to Control Center R5.9 Physical Security for BES Cyber Systems 73.55 Requirements for nuclear personnel who no longer require physical access are covered by CFR. The requirements in R5.9 conflict with the CFR that covers removing physical access for nuclear personnel supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement.Monitoring Physical Access PE-6 E5.8 Monitoring Physical Access R5.10 Physical Security for BES Cyber Systems 73.55 Nuclear personnel are trained and qualified to provide continuous escort for visitors while they are granted physical access to nuclear plants. The requirements in R5.10 are covered by the CFR for nuclear personnel who escort visitors supporting plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R5.11 Physical Security for BES Cyber Systems 73.55 Unauthorized physical access is handled by armed security officers in nuclear security. The requirements in R5.11 are covered by the CFR for unauthorized physical access to the plant where systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R6.1 Physical Access Control Systems 73.55 Physical access control systems are covered by CFR requirements. The requirements in R6.1 are covered by the CFR and this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement. R6.2 Physical Access Control Systems 73.55 Physical access control systems are covered by CFR requirements. The requirements in R6.2 are addressed in the CFR and this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement. R6.3 Physical Access Control Systems 73.55 Physical access control systems are maintained and tested per CFR requirements. The requirements in R6.3 are addressed in the CFR. Therefore, this physical access control system is subject to nuclear cyber security regulation only. Consider exempting nuclear facilities from this requirement.Account Management AC2 D1.2 Account Management R7 Account Management Specifications Consistent with nuclear cyber security plan.Least Privilege AC6 D1.6 Least Privilege R8.1 Account Management Implementation Consistent with nuclear cyber security plan.Account Management AC2 D1.2 Account Management R8.2 Account Management Implementation Duration is inconsistent with nuclear cyber security plan. Requirements should be the same for plant systems whether they support safety, security, EP or BOP.Account

#	Organization	Question 54 Comment
		Management AC2 D1.2 Account Management R8.3 Account Management Implementation Consistent with nuclear cyber security plan. R9.1 Personnel Terminated for Cause Part 2673.56 Duration is inconsistent with nuclear requirements.N/A N/A N/A N/A R9.2 Personnel Terminated for Cause (Control Center) N/A to nuclear - applicable to Control CenterN/A N/A N/A N/A R9.3 Personnel Terminated for Cause (Control Center) N/A to nuclear - applicable to Control CenterAccount Management AC2 D1.2 Account Management R9.4 Access Revocation Duration is inconsistent for removal of access for personnel who no longer require access with nuclear cyber security plan. Requirements should be the same for plant systems whether they support safety, security, EP or BOP. Identification and Authentication (Non-Organizational Users) IA-8 D4.2 Identification and Authentication (Non-Organizational Users) R10.1-5 Account Access Control Specifications The control of passwords contained in R10.1 - 8 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should include the provision contained in note 1 for digital assets that are not technically capable of supporting some of the password requirements. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Least Privilege AC6 D1.6 Least Privilege R10.6 Account Access Control Specifications The control of passwords contained in R10.6 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as Hierarchical permissions.CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Access Enforcement AC3 D1.3 Access Enforcement R10.7 Account Access Control Specifications The control of passwords contained in R10.7 is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as system and security administrative accounts. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by

#	Organization	Question 54 Comment
		nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Separation of Duties AC5 D1.5 Separation of Functions R10.8 Account Access Control Specifications The control of passwords, contained in R10.8, is similar to nuclear requirements. In order to eliminate the possibility of conflicting or dual regulation, CIP standards should contain provision for digital assets that are not technically capable of supporting some of the password requirements such as Hierarchical permissions.CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. The password standards for digital systems that support safety, security, EP or BOP functions should not be regulated differently.Wireless Access AC18 D1.17 Wireless Access Restrictions R11.1 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R11.2 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R11.3 Wireless and Remote Electronic Access Documentation Consistent with nuclear requirements.Remote Access AC17 D.1.1 Access Control Policy and Procedures R12 Wireless and Remote Electronic Access Management 73.5573.56 Duration is inconsistent with nuclear requirements for reviewing remote access. Other physical security and access authorization nuclear regulation ensures personnel who have remote access are trustworthy and reliable therefore this type of review is not justified.N/A N/A N/A N/A R13.1 Remote Access Revocation (Control Center) N/A to nuclear - applicable to Control CenterN/A N/A N/A N/A R13.2 Remote Access Revocation (Transmission) N/A to nuclear - applicable to TransmissionRemote Access AC17 D.1.1 Access Control Policy and Procedures R13.3 Remote Access Revocation Part 26 73.56 Duration is established in nuclear requirements for removal of access for personnel who no longer require remote access.Remote Access AC17 D.1.1 Access Control Policy and Procedures R14.1-3 Wireless and Remote Electronic Access Control Consistent with nuclear requirements.System Use Notification AC8 D.1.8 System Use Notification R14.4 Wireless and Remote Electronic Access Control Inconsistent with nuclear requirements. CIP Standards should acknowledge nuclear programs required by regulation that provide other alternate methods implementing equivalent control consistent with acceptance by nuclear regulators. Add provision for this requirement to be implemented if technically supported.Malicious Code Protection SI-3 E3.3 Malicious Code Protection R15 Malicious Code Consistent with nuclear regulation.N/A N/A

#	Organization	Question 54 Comment
		D5.5 Installing Operating Systems, Applications, and Third Party Software Updates R16.1 Security Patch Management Duration is inconsistent with nuclear regulation otherwise requirements are consistent. D5.5 Installing Operating Systems, Applications, and Third Party Software Updates R16.2 Security Patch Management Consistent with nuclear regulation.N/A N/A D5.4 Hardware Configuration R17 System Hardening Consistent with nuclear requirements.Information System Monitoring SI-4 E3.4 Monitoring Tools and Techniques R18.1 Security Event Monitoring Consistent with nuclear requirements.Information System Documentation SA-5 E6 Defense-In-Depth R18.2 Security Event Monitoring Consistent with nuclear requirements.Incident Monitoring IR-5 E7.5 Incident Monitoring R18.2 Security Event Monitoring Consistent with nuclear requirements.Baseline Configuration CM-2 E10.3 Baseline Configuration R18.4 Security Event Monitoring Duration for maintaining logs is inconsistent with nuclear requirements. The duration for maintaining logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A E6 Defense-In-Depth R18.4 Security Event Monitoring Duration for review of logs is inconsistent with nuclear requirements. The duration for reviewing logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A N/A N/A R19 Communication and Data Integrity in a Control Center N/A to nuclear - applicable to Control CenterBoundary Protection SC-7 E6 Defense-In-Depth R20 Electronic Boundary Protection Consistent with nuclear regulation other than duration. The duration for reviewing alerts and logs for digital systems that support safety, security, EP or BOP functions should not be regulated differently.N/A N/A N/A N/A R21.1 System Boundary Protection N/A to nuclear - applicable to Control CenterBoundary Protection SC-7 E6 Defense-In-Depth R21.2 System Boundary Protection 73.54 Consistent with nuclear requirements. R22 Protective Cyber Systems (duplicate of R14,16,18,23) Duplicate - (duplicate of R14,16,18,23); Remove not neededInformation System Component Inventory CM-8 E10.9 Component Inventory R23.1 Configuration Change Management 73.54 Consistent with nuclear regulation.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.2 Configuration Change Management 73.5450 App B Consistent with nuclear regulation.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.3 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be

#	Organization	Question 54 Comment
		regulated differently.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.4 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be regulated differently.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.4 Configuration Change Management 73.5450 App B Duration is inconsistent with nuclear regulation. Nuclear configuration management programs are mature and are required by 10CFR50 Appendix B. They are implemented for plant digital systems that support safety, security, EP or BOP functions and duration for updating configuration records and documenting changes should not be regulated differently.Configuration Change Control CM-3 E10.4 Configuration Change Control R23.5 Configuration Change Management 73.5450 App B Consistent with nuclear requirements.Baseline Configuration CM-2 E10.3 Baseline Configuration R23.6 Configuration Change Management 73.5450 App B Consistent with nuclear requirements.Information System Component Inventory CM-8 E10.9 Component Inventory R23.7 Configuration Change Management 73.54 Consistent with nuclear requirements.Media Protection Policy and Procedures MP-1 E 1.1 Media Protection Policy and Procedures (SGI, Non-SGI, 2.390) R24.1 Information Protection Consistent with nuclear requirements.Information Output Handling and Retention SI-12 E3.10 Information Output handling and Retention R24.2 Information Protection Consistent with nuclear requirements. R24.3 Information Protection 73.56 The requirements in R24.3 are covered by the CFR for authorization to view security sensitive information for plant systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R24.4 Information Protection 73.56 The requirements in R24.4 are covered by the CFR for unauthorized physical access to the plant where systems performing functions associated with safety, security, emergency preparedness or BOP. Consider exempting nuclear facilities from this requirement. R24.5 Information Protection 73.56 Nuclear personnel are subject to rigorous background checks including criminal investigation, credit investigation, psychological evaluation, random drug screens, etc. to ensure their trustworthiness and reliability. This requirement is not necessary for nuclear personnel. Consider exempting nuclear facilities from this requirement.Media Sanitation MP-6 E 1.6 Media Sanitation and Disposal R25 Media Sanitation Consistent with nuclear requirements.Maintenance

#	Organization	Question 54 Comment
		Personnel MA-5 E4.3 Personnel Performing Maintenance and Testing Activities R26.1 Maintenance Consistent with nuclear requirements.Maintenance Tools MA-3 E4.2 Maintenance Tools R26.2 Maintenance 50 App B Consistent with nuclear requirements.Incident Handling IR-4 E7.1 Incident Handling R27.1 Cyber Security Incident Response Plan Specifications DG-501950 App B50 App E The requirements in R27.1 are covered by the CFR for classifying events as Cyber Incidents whether the plant systems performing functions associated with safety, security, EP or BOP. Plant digital systems that support safety, security, EP or BOP functions should not be regulated differently.Incident Handling IR-4 E7.4 Incident Handling R27.2 Cyber Security Incident Response Plan Specifications 73.54 Consistent with nuclear regulation.Incident Reporting IR-6 N/A N/A R27.3 Cyber Security Incident Response Plan Specifications 73.5473 Appendix GDG 5019 This requirement should be addressed by NRC and FERC/NERC to ensure consistency in reportability requirements.Incident Response Testing and Exercises IR-3 E7.3 Incident Response Testing and Drills R28 Cyber Security Incident Response Plan Testing Specifications 73.54 Nuclear testing of Incident response plans is regulated by site E-Plans. When appropriate, plant digital systems that support safety, security, EP or BOP functions are included and duration for testing these plans should not be regulated differently. Incident Response Policy and Procedures IR-1 E7.1 Incident Response Policy and Procedures R29 Cyber Security Incident Response Plan Review, Update and Communication Specifications 73.5450 App E Duration is inconsistent with nuclear regulation. Nuclear review and updating of Incident response plans is regulated by site E-Plans. When appropriate, plant digital systems that support safety, security, EP or BOP functions are included and duration for testing these plans should not be regulated differently.Incident Response Policy and Procedures IR-1 E7.1 Incident Response Policy and Procedures R30.1 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Contingency Plan CP-2 E8.1 Contingency Plan R30.2 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Recovery and Reconstitution CP-10 E8.6 Recovery and Reconstitution R30.3 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Backup CP-9 E8.5 CDA Backup R30.4 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Information System Backup CP-9 E8.5 CDA Backup R30.5 Recovery Plan Specifications 73.54 Consistent with nuclear requirements.Contingency Plan Testing and Exercises CP-4 E8.2 Contingency Plan Test R31 Recovery Plan Testing Specifications 73.54 Duration is inconsistent with nuclear regulation. Nuclear tests and exercises for recovery for plant digital systems that support safety, security, EP or BOP functions

#	Organization	Question 54 Comment
		should not be regulated differently. R32 Recovery Plan Review, Update, and Communications Specifications Neither nuclear regulation nor NIST 800-53 contain expectations reviews, updates and communication of recovery plans at the frequencies established by R32. The bases for R32 requirements are unclear and consideration should be given to removing it.

END OF REPORT