Name (59 Responses)
Organization (59 Responses)
Group Name (36 Responses)
Lead Contact (36 Responses)
Question 1 (85 Responses)
Question 2 (85 Responses)
Question 3 (85 Responses)
Question 4 (83 Responses)
Question 5 (84 Responses)
Question 5 Comments (95 Responses)
Question 6 (84 Responses)
Question 7 (84 Responses)
Question 8 (0 Responses)
Question 8 Comments (95 Responses)
Question 9 (0 Responses)
Question 9 Comments (95 Responses)
Question 10 (0 Responses)
Question 10 Comments (95 Responses)
Question 11 (0 Responses)
Question 11 Comments (95 Responses)
Question 12 (0 Responses)
Question 12 Comments (95 Responses)
Question 13 (0 Responses)
Question 13 Comments (95 Responses)
Question 14 (0 Responses)
Question 14 Comments (95 Responses)
Question 15 (77 Responses)
Question 15 Comments (95 Responses)
Question 16 (0 Responses)
Question 16 Comments (95 Responses)
Question 17 (0 Responses)
Question 17 Comments (95 Responses)

Individual
David Proebstel
Clallam County PUD No.1
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Individual
Michelle R D'Antuono
Ingleside Cogeneration LP
No
Yes
Yes
Yes
Yes
Yes
Yes
For the most part, Ingleside Cogeneration LP supports the transition of asset-based cyber protection to one based on BES Cyber Systems. The concept reflects the fact that attackers look to compromise distributed systems, not necessarily individual components. A system-based approach should capture weaknesses that are not obvious when looked at in piece-part. However, we are concerned with the elimination of redundancy as a consideration as required in the definition of BES Cyber Asset. It includes a statement that the redundancy of "affected Facilities, Systems, and equipment shall not be considered when determining adverse impact." As a time tested way to preserve reliability, we don't see why such a technique can be dismissed out of hand. Ingleside Cogeneration fully understands that a cyber attack may simultaneously compromise multiple systems, but there are methods to reduce the risk – for example, by using redundant systems using fundamentally different programmable components/schema. Every tool in the toolbox must be available. However, the definition as written provides an economic disincentive to use redundancy to protect against cyber intrusions. We don't believe this is the drafting team's intent, and we recommend the sentence be removed.
Group
Northeast Power Coordinating Council
Guy Zito
No
Yes
Yes
Yes
Yes
No
No
For clarity, suggest changing the BES Cyber Asset definition from "it is directly connected to a Cyber Asset within an ESP" to "it is directly connected to a network, or to a Cyber Asset within an ESP".

Request clarification on the definition of EAP. Must it be routable protocol on both sides?
The definition of Reportable Cyber Security uses the terms "compromised" and "disrupted" plus the phrase "reliability tasks of a functional entity". All three need their own definition/clarification.
No
Although the proposed Version 5 Implementation Plan states that “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan,” there are concerns that need clarification. The concerns refer to the transition from the currently effective Version 3, through Version 4 and finally to Version 5. Given that (a) the Version 4 Standards and associated Implementation Plan were recently approved by FERC; (b) the proposed Version 5 Implementation Plan contains a minimum 24-month period for enforcement means that there will be a period of time during which Version 4 would be effective; and (c) when Version 4 becomes effective there will be newly identified CAs that will have to be made compliant. In order to comply with Version 4 requirements, entities will be need to allocate funding and resources to perform work necessary to become compliant at newly identified facilities. Much of this work must be performed in anticipation of the enforcement date. Once Version 5 becomes effective, application of the proposed categorization of BES Cyber Systems may very well result in much of the work done for Version 4 compliance being in the end unnecessary. Request clarification on the Disaster Recovery's "completion of the restoration activities" (top of the clean version's page 5). What event/action/etc. signifies this completion?
Section 5 for CIP-003-5 is the only place that explains how to read the bullets and numbers in the Measures. From the second paragraph of Section 5, "Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence." Request clarification this bullets and numbers explanations applies to the Requirements and Applicability sections of each of CIP-002-5 - CIP-011-1. If this was the SDT's intent, then recommend this clarification be added to Section 5 of each of CIP-002-5 - CIP-011-1. General comment--recommend that each Requirement’s Part identify that Part’s goal.
Individual
Frank Dessuit
NIPSCO
No
Yes
Yes
Yes
No
No
No
We agree with the new definitions of BES Cyber System and BES Cyber Asset. However, NIPSCO requests what is the definition of “programmable” electronic device and what is included in such device. In addition, it is recommended that the word “data in those devices” be removed from the description.
NIPSCO requests further review of the description and recommends that the description should include a defined list of what is included in the PSP
NIPSCO requests elimination of “Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants” from the definition of Interactive Remote

Access.
NIPSCO request the addition BES Cyber Asset be added to the scope of the ESP definition. . NIPSCO requests that the term “cyber system” be changed to a “cyber asset,” to the scope of the external routable connectivity definition.
NIPSCO requests further clarification on what is meant by an, “attempt to disrupt” and an “attempt to compromise” as it is applied to an event and how to show evidence of such intent. NIPSCO recommends to use either “compromises” or “confirmed attempt to disrupt,” to replace attempt to disrupt and attempt to compromise. NIPSCO request clarification for “reliability tasks”. Are they the same reliability tasks as required by PER-005?
Yes
Individual
Roger Dufresne
Hydro-Québec Production
Yes
Yes
Yes
Yes
Yes
No
Yes
"Protected cyber asset" definition is hard to understand and confusing. Clarification should be done with a more concise ans structure statement.
Group
Comment Development SME List
Gerald Freese
No
Yes
Yes
Yes
No
Yes
Yes
(1) BES Cyber Asset - The third sentence states "Each BES Cyber Asset is included in one or more BES Cyber Systems." This statement adds no additional substance to the definition. It should be removed and placed into guidance for determining BES Cyber Systems. 2) BES Cyber System – The definition is not clear as to whether the BES Cyber Assets need to be connected to and/or interact

with each other to be considered a BES Cyber System. For example, would a group of 6 protective relays in the field that are all performing protection functions for a generating unit be considered a BES Cyber System if they are not connected together.
1) Intermediate Device – The second sentence should be removed from the definition. The second sentence is stating a required architectural design. If it is a required design then it should be covered in a requirement and not stated in a definition; we recommend adding the statement to a requirement in CIP-005.
Yes
(1) BES Cyber Asset - The third sentence states "Each BES Cyber Asset is included in one or more BES Cyber Systems." This statement adds no additional substance to the definition. It should be removed and placed into guidance for determining BES Cyber Systems. (2) BES Cyber System – The definition is not clear as to whether the BES Cyber Assets need to be connected to and/or interact with each other to be considered a BES Cyber System. For example, would a group of 6 protective relays in the field that are all performing protection functions for a generating unit be considered a BES Cyber System if they are not connected together. (1) Intermediate Device – The second sentence should be removed from the definition. The second sentence is stating a required architectural design. If it is a required design then it should be covered in a requirement and not stated in a definition; we recommend adding the statement to a requirement in CIP-005.
Individual
Michael Falvo
Independent Electricity System Operator
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Steven Powell
Trans Bay Cable
No

Yes
Yes
No
No
Data Centers need to be definded. This term was added in CIP V5 and a definition should be provided to ensure consistancy across all RC's
Yes
Yes
Add definition for data center
No
No address of CIP V4 was made
Group
Southwest Power Pool Regional Entity
Emily Pennel
No
Yes
No
No
Yes
No
No
The definition of Cyber Asset ignores data in motion. The definition either needs to drop the added language “in those devices” or add language regarding data both at rest and in motion.
No
The definition of CIP Exceptional Circumstances includes the condition “an imminent or existing hardware, software, or equipment failure.” This language essentially eliminates the need for conducting a personnel risk assessment and Cyber Security training for vendor support staff. The condition needs to be modified to permit the exceptional circumstance only in the event of a failure requiring vendor support from personnel that do not routinely support the impacted system. The idea is that the call center technical support team (such as from Cisco or Oracle) could provide support in an exceptional circumstance but routine support from, for example, an EMS vendor would require the support staff to have been pre-trained and pre-screened.
Physical Access Control Systems need to include the workstations used to provision access rights and to monitor alarms. The Physical Security Perimeter needs to include the qualification “capable of deterring unauthorized physical access.” A gate and climbable fence do not deter unauthorized access and should not be considered a physical border for the purposes of the definition.
No
The Electronic Access Point definition needs to say “allows or is capable of allowing” routable communication in order to pick up a dual-homed Cyber Asset, including laptops with wireless not hardware-disabled. The External Routable Connectivity needs to consider inside-to-outside connectivity and not just outside-to-inside connectivity.
Reportable Cyber Security Incident needs to include an incident that has compromised or disrupted a

BES Cyber System whether or not the reliability tasks of a functional entity have been compromised or disrupted. Otherwise, entities will argue that redundancy eliminates the need to report because the ability to fail over to a backup system means operations was not disrupted.
No
The requirements of CIP-005-3 R2 are not sufficiently unique or complex as to warrant an additional year to implement. Responsible Entities will be able to leverage their High and Medium impacting controls to apply to the Low Impacting systems. Additionally there is no reason why the first instance of a requirement cannot be performed within the two year preparation time prior to the effective date of the standards. Why would you allow, for example a year after the effective date of the standards to conduct the first training or to verify that provisioned access is correct?
None
Individual
Thomas A Foreman
Lower Colorado River Authority
Yes
Yes
Yes
Yes
Yes
Yes
No
Change the definition for Cyber Security Incident as follows: Cyber Security Incident Any A malicious act or suspicious event that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System.
Yes
Individual
Glen Sutton
ATCO Electric
Yes
Yes
Yes
Yes
Yes
CIP-002 provides examples or Electronic access control and monitoring systems as well as Physical access control systems. These could be removed from CIP-002 and added to the definitions for these defined terms
Yes
Yes

Yes
Group
NRG Energy Companies
Alan Johnson
No
No
Yes
Yes
Yes
No
No
The BES Cyber system classification should be empirically clear to correlate the facility impact rating criteria per CIP-002-5 Attachment 1 with the classification of impact of associated BES systems within that facility. For example, a high impact facility must classify the BES systems as only high impact.
1. Definition is incomplete with the inclusion of BES Cyber Assets/Systems. Proposed new definition of Control Center: “One or more facilities hosting BES Cyber Assets/Systems including operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of:…….” 2. In addition, the threshold for control centers at generation facilities exceeding 300MWs and under 1500MWs, as written, is classified as medium impact. This classification should exclude those facilities that provide control of remote sites such as gas turbines. Generally these remote sites would be considered low impact facilities but due to the central dispatch, these sites automatically are classified as medium impact facilities. Please clarify. 3. The generation control center definition should further delineate if the BES systems are shared or not. There are scenarios that exist with more than one entity dispatched from one center and no shared BES system exists between the entities. This should not result in inclusion as medium impact risk to the BES as currently written.
Does the definition of ESP presume the presence of an Electronic Access Point? In other words, does a BES Cyber System with no External Routable Connectivity fall within the scope of the CIP standards? Clarifying this point will pre-empt the need for interpretation or a CAN later.
Cyber Security Incident – remove the words “or suspicious event”. Suspicious is too vague and subject to interpretation. Suggest the definition be changed to: “A malicious act that (1) Compromises, or was an attempt to compromise a BES Cyber System, and (2) Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.”
Yes

Individual
Martyn Turner
LCRA Transmission Services Corporation
Yes
Yes
Yes
Yes
Yes
Yes
No
Change the definition for Cyber Security Incident as follows: Cyber Security Incident Any A malicious act or suspicious event that: • Compromises the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or, • Disrupts the operation of a Critical Cyber Asset BES Cyber System.
Yes
Individual
Jianmei Chai
Consumers Energy Company
No
Yes
Yes
Yes
Yes
Yes
Yes
BES Cyber Asset - The definition of BES Cyber Asset continues to remain vague. Although CIP-002 and the SDT have made progress toward creating “bright-line” evaluation criteria in the standard and Attachment I for Facilities, Systems and equipment, by using the phrase “adversely affect the reliable operation” in the definition, the BES Cyber Asset definition continues from Draft #1 to not provide bright-line criteria. BES equipment is frequently removed from operation with no reliability effect, yet would be in-scope in the proposed standard. In addition, not all BES facilities, systems and equipment, nor cyber/programmable devices, are of the same value or importance of function. In the proposed standard, a configurable electronic panel meter (providing local, seldom-used indication) in a substation, would rise to the same level of compliance as an RTU or protective relay in that same substation. In this regard, we recommend that the SDT consider developing bright-line criteria that could be used for defining BES Cyber Assets at different levels based on the asset’s impact of MW levels, system disturbance potential, or other substantial BES events. In Attachment 1, Section 2, (and especially item 2.5) the SDT seems comfortable eliminating applicability for facilities of lower voltages or MW value. It would seem foolish to then include cyber assets at other facilities, if the impact on reliability due to a compromised cyber asset was small.

No
Page 5 of the clean version Implementation Plan states “The following security requirements in CIP-003 through CIP-011 apply to …..”, however, there is no CIP-003 requirement included. Please correct as needed. Several Implementation Plan associated requirements (e.g. CIP-003-5 R2.4, CIP-007-5 R7.2, CIP-010-1 R3.1 & R3.3, etc.) need to be revised before they could have appropriate implementation schedule.
Individual
Joe Petaski
Manitoba Hydro
Yes
No
No
No
Yes
Yes
Yes
We suggest adding the word “NERC certified” before “operating personnel”.
It is not clear what the “unauthorized distribution” mean. Authorized distribution should be clarified.
Given that the handling of a PACS alert could be a cell phone, an email server or a PC, it doesn’t mean they become the PACS. Only the computer that initiates the alert should be considered part of the PACS. We suggest changing “alert” to “initiate alerts”.
No
Individual
Michael Schiavone
Niagara Mohawk (dba National Grid)
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
We recommend adding definition of “annual” to the definitions document. The definition should be “once per calendar year”.
Individual
Michael Jones
National Grid
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
We recommend adding definition of “annual” to the definitions document. The definition should be “once per calendar year”.
Individual
Jonathan Appelbaum
United Illuminating company
Yes
Yes
Yes
Yes
No
UI believes that Electronic Access Control or Monitoring System this is limited to the firewall appliance that gathers traffic information and enforces the ruleset. Informally UI has heard that this term is meant to include or log monitors and gathering appliances, any devices that analyze logs and generate alerts, the password servers, and it applies to both remote access communication and individual log ons. The scope should be narrowed to all the controls around the firewall appliance.
Yes

Yes
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments
Yes
UI Agrees with EEI Consensus comments
UI Agrees with EEI Consensus comments. In addition Ui would appreciate the incorporation of allowable defects and corrections in the implementation of the CIP program. NIST does allow a security program to identify and self-correct errors as a control. UI would also like the introduction of escorted electronic access via WEBEX remote sessions to allow for SCADA support, maybe limited to Medium assets. We also believe the Standards force each SCADA support Vendor to take each entity's training program when this is very inefficient.
Group
Arizona Public Service Company
Janet Smith
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Alice Ireland
Xcel Energy
Yes
No
No
Yes
Yes
Yes

No
For item 4) we suggest that the intent needs to be made clear that this applies to BES assets, and that location should be defined. We propose the following revision: “…4) a Generator Operator for BES generation Facilities at two or more locations. A location is defined as a separate property with a continuous physical boundary.”
The definition of CIP Exceptional Circumstances has been changed to include “an imminent or existing hardware, software, or equipment failure…” As written, this is far too broad (for example, as written, each time we have a single asset fail we could declare an Exceptional Circumstance). At a minimum, this phrase should be re-written to narrow its scope or, even better, stripped out entirely from the definition.
The definition of cyber security incident now includes “Physical Security Perimeter.” This is a significant change in the definition of a cyber-security incident and the impact will be difficult to assess. The definition is also narrowed to “Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter” or “Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.” Disruption is not defined and it is unclear if non-malicious “disruptions” are excluded.
Yes
Group
PNGC Comment Group
Ron Sporseen
Yes
No
Yes
Yes
Yes
Yes
Yes
Control Center – NRECA is concerned that in this definition the mere presence of a SCADA HMI might be considered a Control Center by a CEA if it could possibly be used to control BES assets in real-time even if an entity does not use it that way. Some of the registered entities do not man these control centers 24/7 and are unable to perform real time control after hours, or any other time that other duties take them 15 minutes away from the computer. In some instances these entities might be registered as TOPs only because they own a limited and discrete 115 kV facility that no other entity was willing to register as a TOP for. Often times this 115 kV facility performs no reliability function. NRECA suggests adding “24/7 to the first sentence of the Control Center definition as shown in the underlined text: “One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …”
CIP Senior Manager – In this definition replace “CIP Standards” with CIP-002 through CIP-011. If this is not completed, this definition would apply to CIP-001 which still exists and is an unrelated standard. This revision will provide clarity to the limit of the definition.

Yes
Individual
John Souza
Turlock Irrigation District
Yes
Yes
Yes
Yes
Yes
No
Yes
In the definition of an ESP, we believe that "BES Cyber Systems" should be changed to "BES Cyber Assets" because entities are allowed to group such Assets into Systems at their discretion and the grouping they select may result in a particular ESP surrounding only a portion of a System and other ESPs surrounding the remaining portions of the System.
No
See question 16 comment
Although we agree with the Implementation Plan in general, we believe that the last section of the Plan which contains a table showing which Requirements apply to Associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets is redundant and should be removed. The Standards already contain this information in a more granular form (at the sub-part level). If the table remains as part of the Implementation Plan then it should include the same granularity of the Standards. Also, there are a number of errors in the table, such as: (1) the introductory sentence states “CIP-003 through CIP-011” however, CIP-003 is not part of the table, (2) CIP-005 has one part (part R1.2) which is applicable to Protected Cyber Assets but is not listed in the table, (3) CIP-009 has various Requirements which are missing from the table.
In all places where the statement “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and ....” should be revised now that CIP Version 4 has been approved by FERC. We would like to thank and applaud the members of the SDT for the work they have done, especially for the work involved in this second draft.
Individual
Chris Higgins on behalf of BPA CIP Team
Bonneville Power Administration
No
Yes
No
Yes
No
No

No
BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.) Regarding the BES Cyber System: BPA has no comments. Cyber Asset: Facilities, Systems, or equipment which if destroyed, degraded, or otherwise rendered unavailable when needed, would prevent the responsible entity from maintaining the reliable operation of the BES. (e.g. criteria specified in CIP-002-5, Attachment 1 - Impact Rating Criteria)
Regarding BES Cyber System Information: BPA believes the definition is acceptable, it could be made clearer by breaking the second sentence into a list, as in limited to: Security procedures developed by the responsible entity; Security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; Collections of network addresses; or Network topology of the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, and not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Regarding CIP Exceptional Circumstances: It is often impossible to determine the outcome of a situation until after the fact. BPA recommends: A situation that involves or threatens to involve more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability. Regarding CIP Senior Manager: BPA has no comments.
Regarding Electronic Access Control and Monitoring Systems: BPA has no comment. Regarding Interactive Remote Access: BPA thinks that including "Interactive remote access does not include system-to-system process communications." is appropriate and has concerns with the other parts of this definition. In particular, BPA believes that trying to list all the possibilities is confusing and unnecessary. BPA suggests the following rewording: Interactive Remote Access: All human-initiated routable or dial-up access 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). (Ownership of the Cyber Asset used to initiate Remote Access is not relevant to the definition of Remote Access.) Interactive remote access does not include system-to-system process. Regarding Intermediate Device: The second sentence states an unnecessary requirement that would not increase the security of the systems NERC CIP is intended to protect. BPA believes it should be deleted.
Regarding Electronic Access Point: BPA has no comment. Regarding Electronic Security Perimeter: BPA has no comment. Regarding External Routable Connectivity: BPA believes that "External Routable Connectivity" should only apply if the routable connection goes all the way to the BES Cyber Asset. Since this has been a topic of concern in the past, BPA suggests the following revision: External Routable Connectivity: A BES Cyber System that is accessible from a Cyber Asset that is outside the BES Cyber Asset's associated Electronic Security Perimeter via a bi-directional routable protocol connection terminating at a BES Cyber Asset that is part of the BES Cyber System. Regarding Protected Cyber Asset: As stated, the definition would cause maintenance devices such as handheld cable testing devices to be included as Protective Cyber Assets, even if they were only connected to the network for a few seconds. At the same time, BPA realizes that any network device poses a higher risk than a directly connected device. BPA suggests the following revision: A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter (A Cyber Asset is not a Protected Cyber Asset if it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes and it is directly connected to a Cyber Asset within an ESP or to a BES Cyber Asset for 30 consecutive calendar days or less, or used for such purposes and connected for less than 30 days to a routable network within an ESP protecting BES Cyber Assets.).
Regarding Cyber Security Incident: BPA recognizes that the proposed definition combines two

separate types of incidents; a cyber incident and a physical security incident. Unauthorized physical access into a physical security perimeter does not automatically lead to a “cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, miss-operation, or non-operation, adversely impact one or more Facilities, Systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.” Unauthorized entry or access to a facility containing such cyber assets can be one of many types of incidents; burglary, theft, or inadvertent circumvention of a policy, practice or system. Thus it would be classified as a physical security incident and handled accordingly and not as a Cyber Incident. Combining the two events together will potentially lead to the false classification and analysis of events. BPA believes that Physical Security Incidents should be a separate category of incident, and only when a physical security incident is shown to be related to an attempt to disrupt the BES should it be examined in context of a cyber security incident, and only if there are indications of a cyber security nexus. Regarding Reportable Cyber Security Incident: BPA believes this definition is too open. Many events may compromise or disrupt one or more reliability tasks and may not be caused by a person, not be done with malicious intent and in the end, not be determined to be a cyber security issue at all. Suggested Change: Any Cyber Security event that has compromised or disrupted one or more reliability tasks of a functional entity, which through investigation and escalation, has been determined by the Responsible Entity to be reportable to ES-ISAC.
Yes
Individual
Benjamin Beberness
Snohomish County PUD
No
No
Yes
No
Yes
Yes
Yes
BES Cyber Asset, BES Cyber System, and Cyber Asset: The draft CIP versions 5 Reliability Standards are very BES definition centric. Due to the proposed changes to the BES definition it is very difficult for the electric industry to comment on a standard as it is unclear if the currently or proposed BES definition will be applied. This change in the definition could significantly change the applicability of the version CIP Reliability Standards. Although it is clear the SDT has made attempts to size the applicability of the CIP version 5 requirements with the size of the registered entity, the current draft will cause significant resource burdens on facilities that have demonstrated they cannot impact the reliability of the Bulk Electric System. As a Transmission Dependent Utility SNPD supports a reliable system because we are at the end of the system and SNPD’s customers are exposed to all disturbances on the main grid. However SNPD also support efficiency and spending significant resources with little to benefit is not beneficial to the reliability of the BES or to the Level of Service (“LOS”) SNPD provides its customers. Control Cente: SNPD disagrees with the CIP-002-5, 2.11 as it dictates that all registered Balancing Authorities and Transmission Operators are automatically assigned a Medium Impact Rating (M). There are many very small Balancing Authorities and Transmission Operators that have little to no reliability impact to neighboring systems and should not be included as a medium impact rating. In addition the assigned registration as a TOP is extremely subjective. The NERC Statement of Compliance Registry Criteria (“SCRC”), section III (d), uses the same criteria to define both Transmission Owner (“TO”) and Transmission Operator (“TOP”) . In addition, the application of this criteria, especially as to under what circumstances an entity is a TO and not a TOP is not defined and is not consistent through the regions. SNPD supports removing section 2.11 as there is no “reliability based” justification that registration as TOP justifies a Medium

Impact Rating.
The draft CIP versions 5 Reliability Standards are very BES definition centric. Due to the proposed changes to the BES definition it is very difficult for the electric industry to comment on a standard as it is unclear if the currently or proposed BES definition will be applied. This change in the definition could significantly change the applicability of the version CIP Reliability Standards. Although it is clear the SDT has made attempts to size the applicability of the CIP version 5 requirements with the size of the registered entity, the current draft will cause significant resource burdens on facilities that have demonstrated they cannot impact the reliability of the Bulk Electric System. As a Transmission Dependent Utility SNPD supports a reliable system because we are at the end of the system and SNPD’s customers are exposed to all disturbances on the main grid. However SNPD also support efficiency and spending significant resources with little to benefit is not beneficial to the reliability of the BES or to the Level of Service (“LOS”) SNPD provides its customers.
The draft CIP versions 5 Reliability Standards are very BES definition centric. Due to the proposed changes to the BES definition it is very difficult for the electric industry to comment on a standard as it is unclear if the currently or proposed BES definition will be applied. This change in the definition could significantly change the applicability of the version CIP Reliability Standards. Although it is clear the SDT has made attempts to size the applicability of the CIP version 5 requirements with the size of the registered entity, the current draft will cause significant resource burdens on facilities that have demonstrated they cannot impact the reliability of the Bulk Electric System. As a Transmission Dependent Utility SNPD supports a reliable system because we are at the end of the system and SNPD’s customers are exposed to all disturbances on the main grid. However SNPD also support efficiency and spending significant resources with little to benefit is not beneficial to the reliability of the BES or to the Level of Service (“LOS”) SNPD provides its customers.
No
Group
PPL Corporation NERC Registered Affiliates
Stephen Berger
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

1.) PPL Affiliates recommend addition of definitions of “Impact” and “Adverse” in regards to CIP-002 (BES Adverse Reliability Impacts). 2.) PPL Affiliates recommend the addition of a definition for “Common Control System” in regards to CIP-002 Attachment 1, Section 2.10.
Individual
Larry Watt
Lakeland Electric
No
No
Yes
No
No
"Please see comments submitted by FMPA through the formal comment process."
No
No
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
Yes
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
Individual
Ron Donahey
Tampa Electric Company
No
Yes
Yes
Yes
Yes
Yes
No
Tampa Electric recommends that the SDT improve the definition of the BES Cyber Asset, Cyber System, and Cyber Assets related to “adversely impact” one or more BES Reliability Operating Services in order to provide clarity. The current NERC Glossary of Terms used in NERC Reliability Standards shows: Adverse Reliability Impact (BOT Approved: 2/7/2006 FERC Approved: 3/16/2007 [Archive] The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection. Adverse Reliability Impact (BOT Approved: 8/4/2011 FERC has not approved) [Archive] The impact of an event that results in Bulk Electric System instability or Cascading.
BES Cyber Asset – • redundancy shall not be considered - does this go against the basic tenets of system planning? How does this affect subs when load is automatically re-routed: • 30 consecutive calendar days or less – what does this mean? Are we talking about USB connected devices? Why not spell out qualified devices, e.g., non-cyber devices, laptops, etc. External routable connectivity – do

we need a definition of routable? Intermediate device – what security is required for the intermediate device? Does this leave a risk that entities might leave it on the corporate network? Transient cyber asset –check ‘final’ (remove redline)
The SDT should consider definitions should reflect the language in the OE-417 to enable entities to comply with both sets of requirements.
Yes
Tampa Electric suggests that the SDT review the table on the pp. 5-6 for security requirements that apply to EACMs, PACS, or Protected Cyber Assets. We noted that there may be discrepancies for the determination of what applies to which systems.
Tampa Electric appreciates the efforts of the Standards Drafting Team, NERC, and Registered Entities in the development of version 5 of the CIP standards.
Individual
Annette Johnston
MidAmerican Energy Company
No
No
No
No
No
Yes
No
(1) BES CYBER ASSET: The word “Systems” should not be capitalized. “Systems” is not a defined term. (2) BES CYBER SYSTEM: No comment. (3) BES SITES: In conjunction with our CIP-002 comments, we propose a new definition be created for BES Sites. Substations 100kV and above, generating units above (insert # to set the floor) MW (MVA?), control centers and backup control centers used by NERC certified operators to support the real time operations of the interconnected Bulk Electric System, Blackstart Resources, Cranking Path and initial switching requirements. [Note to SDT: The lists are based on existing lists entities need for Operating and Planning Reliability Standards applicable to their NERC registration criteria.] Consider also if “BES CIP Sites” would be better to reserve the definition solely for CIP and avoid future possible issues or confusion with Operations and Planning Reliability Standards. (4) CYBER ASSET: No comment.
(1) CONTROL CENTER: V5 creates a CIP-specific definition of Control Center. CIP standards are not the only NERC standards using the term. The CIP definition does not fit the context of the other NERC standards. Multiple definitions across reliability standards for the same term are confusing to implement and complicate auditing. The 300 MW threshold in the proposed V5 definition has little basis relative to reliability. Control center should remain undefined in the CIP V5 standards and all references should be lower case. Create a separate project for creation of a definition that would apply across all NERC standards – consistent with strategy for one of EEI’s key issues.
(1) BES CYBER SYSTEM INFORMATION: MidAmerican Energy would support the revised definition, if the following sentence was removed from the definition and put into guidelines: “Examples of BES Cyber System Information may include, but are not limited to, security procedures developed by the responsible entity and security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.” (2) CIP EXCEPTIONAL CIRCUMSTANCES: We appreciate revisions made to the definition to allow “similar conditions.” The SDT added “an imminent or existing hardware, software, or equipment failure” in response to comments. This seems to introduce issues with other requirements. For example, equipment failures covered by this definition likely would lead to invoking the CIP-009 recovery plan. CIP-009 R1.5 requires processes to preserve data, except for CIP Exceptional Circumstances. Based on the revised definition of CIP Exceptional Circumstance, CIP-

009 R1.5 would never be required in the case of an equipment failure. (3) CIP EXCEPTIONAL CIRCUMSTANCES – USE IN THE STANDARDS: There is a lack of clarity within the standards regarding use of CIP Exceptional Circumstances, since there is not one requirement like there was in version 4 for exceptions. By specifically mentioning CIP Exceptional Circumstance in only certain requirements, does that mean it cannot be used in any requirements where it is not mentioned? The guidance on CIP-003 R1.10 is confusing. (4) CIP SENIOR MANAGER: No comments.
(1) PHYSICAL ACCESS CONTROL SYSTEMS: No comments. (2) PHYSICAL SECURITY PERIMETER: The definition is contradictory to the applicabilities throughout the standards. For example, medium impact BES Cyber Assets or Systems without external routable connectivity do not require a PSP. This issue would be resolved with the following suggested text: “the physical border surrounding locations in which applicable Cyber Assets reside, and for which access is controlled.”
(1) ELECTRONIC ACCESS CONTROL OR MONITORING SYSTEMS: The glossary term should be Electronic Access Control Systems to be consistent with the glossary term Physical Access Control Systems. Introduction of the word “perform” creates confusion. Introduction of “or BES Cyber Systems” creates confusion and potentially expands the scope. We propose the following: “Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s).” (2) INTERACTIVE REMOTE ACCESS: The definition is contradictory to requirements, since the definition currently refers to dial-up access but dial-up assets are not required to be in an ESP. We suggest the following revised introductory sentence: “All routable user-initiated 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), using a client or remote access technology.” Delete “whether routable or dial-up.” (3) INTERMEDIATE DEVICE: The definition should be revised to allow application proxy firewalls. The following is proposed: “A Cyber Asset or collection of Cyber Assets that restrict Interactive Remote Access to only authorized users. The Intermediate Device may terminate on an EAP or be external to the ESP.”
We do not have any comments on these four terms.
(1) CYBER SECURITY INCIDENT: No comments. (2) REPORTABLE CYBER SECURITY INCIDENT: The revised definition is not clear due to the use of “reliability tasks,” which is not defined or explained. We suggest this definition be an extension of Cyber Security Incident. Cyber Security Incidents include attempts, which should not be reportable. The following is proposed as the definition for Reportable Cyber Security Incidents to clearly distinguish the difference that an event must actually have compromised or caused a disruption to be considered reportable: “A Cyber Security Incident that compromised the ESP or PSP or disrupted the operation of an applicable BES Cyber Asset or low BES Site.” (3) In Order 706, paragraph 660, FERC directed the ERO to provide guidance regarding what should be included in the term “reportable incident.” The directive was for guidance, and not for this information to be included within the standard itself. Since there is no guidance for definitions, we suggest additional information and examples of Reportable Cyber Security Incidents be provided in the CIP-008 guidelines and replace the fourth paragraph in guidance for R1.
No
(1) INITIAL PERFORMANCE REQUIREMENTS: CIP-009 R1.4 refers to verifying “initially” after backup. We have proposed revised text for this requirement to remove the term “initially.” If this is not changed, the implementation plan should make it clear that entities do not have to complete this requirement until backup is performed. (The term “initially” does not refer to the initial implementation of V5.) (2) CIP-010 R3.2 is a 36-month requirement, so the initial performance should not be required in 12 months. Change the initial performance to 36 months. (3) TRANSITION FROM V4 TO V5: The following statement makes it sounds like V4 will not become effective: “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective.” Remove this language and reconsider the July 15 references. There is now an order to implement V4. V4 was approved by FERC on April 19, 2012. V4’s effective date is April 1, 2014 (first day of the eighth calendar quarter after approval.)
(1) KEY ISSUES TO ADDRESS: MidAmerican Energy is committed to helping find solutions that will result in timely industry approval of V5, and we welcome the opportunity to discuss the key issues and solutions with the drafting team. MidAmerican Energy feels several key issues must be addressed to achieve industry approval with draft 3 and meet the targeted schedule. These issues have been discussed with other entities through EEI and other industry groups. We have incorporated details on

most of these issues and proposed solutions throughout our comments, but also provide a summary here. (a) Issue: Low Impact BES Cyber Assets in scope. There is an audit issue of providing evidence of policy implementation on low impact Cyber Assets. Solution: As discussed in our CIP-002 comments, we support the MRO NSRF’s proposed revisions to CIP-002 that provides a solution to this issue. The CIP-003 R2 requirement would be applied to CIP Sites, not individual Cyber Assets. (b) Issue: Inclusion of Cyber Assets regardless of connectivity. Solution: Add External Routable Connectivity as a qualifier in the applicability column for more requirements throughout the standards. Many types of industrial control type Cyber Assets have very limited capability for a number of the CIP requirements and are generally a low security risk as an attack vector when they do not have External Routable Connectivity. Focus industry resources on higher risks and select requirements for the addition of External Routable Connectivity where these devices will generate TFEs and/or violations if TFEs are not available. (c) Issue: Zero-defect requirements with compliance (not reliability) risk. Solution: The statements for the requirements above the tables require implementing the elements of the table. Add language in the statement for the requirement above the table to incorporate the concepts of continuous improvement, such as: “The Responsible Entity shall measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations, per se.” NIST 800-53 Appendix E minimum assurance requirements for security controls emphasize continuous improvement, expect “expeditious” correction (“timely” for lows) and do not expect perfection. It is also proposed in response to FERC’s order on find, fix and track. In paragraph 81, FERC asked industry for proposals to revise or remove requirements to focus resources on serious risks to reliability. It also aligns with preliminary efforts to move toward more risk based auditing. (d) Issue: Complexity of Applying the Requirements. There are approximately 20 applicability variations, which makes it complicated to map the requirements to the specific classification of assets. Solution: MidAmerican Energy has created an Excel spreadsheet tool to use in analyzing the applicability variations. This spreadsheet has been provided separately to the SDT. The spreadsheet could be used as the starting point to produce a comprehensive mapping of each classification of asset, including all applicable requirements in a single document. The mapping document should be posted with draft 3 to demonstrate how an entity would actually apply the requirements. It is a final check before approval that the requirements are in sync across all standards and a valuable tool for entities to use in implementation. (e) Issue: Blackstart units and cranking paths moved to Low Impact. Solution: Provide sufficient technical and risk-based justification to support regulatory approvals of this key issue. (f) Issue: Immediate revocation of access. V5 requires that the revocation process be initiated immediately and completed within 24 hours. FERC Order 706 directed “immediate” revocation. However, BES Cyber Systems are categorized now taking risk into account. Solution: Limit to high impact Cyber Assets only. Allow reasonable response time for medium impact and protected information, for example, retain V4 timing. In addition, CIP-004-5 R7 is a candidate for the proposed continuous improvement language in the requirement section. See c) above. (g) Issue: Physical Access Controls for High Impact. Many in the industry question if two different control systems are required. Solution: Clarify in CIP-006-5 R1.3 that two authentication methods using the same control system are compliant, for example badge and PIN or bio and PIN or badge and bio. (h) Issue: Violation Risk Factors. One VRF is assigned to a requirement, regardless if it applies to both high and medium impact. Solution: Where a medium VRF is proposed, revise it to medium for high impact and lower for medium impact. Change some mediums to lower. NERC’s VRF summary table needs to be flexible enough to accommodate the arrival of categorization without driving multiple requirements just to reflect different VRFs that correspond to different impact categories. (i) Issue: Definition of Annual. Annual is not in the NERC glossary. CAN-0010 establishes once per calendar year (unless the entity elects the tighter period of once within a 12-month period). V5 is more restrictive than the CAN and creates a second criterion for reaching compliance in 12 requirements. V5 creates a CIP-specific meaning of annual that is different than other standards. Solution: Use “annual” in V5 references, or use “once per calendar year or a period not to exceed 15 calendar months between occurrences.” This proposal is not more restrictive than CAN-0010 and provides entities with more workload scheduling flexibility. (j) Issue: Definition of Control Center. V5 creates a CIP-specific definition of Control Center. CIP standards are not the only NERC standards using the term. Solution: Do not include a definition of control center in V5, but create a separate project for creation of a definition that would apply across all NERC standards. (k) Issue: PSP Monitoring and Alerting for entire PSP. Solution: MidAmerican Energy has provided suggested text to allow entities to monitor only access points into the PSP, if a six-wall border is established. (2) GUIDELINES: Due to the extensive amount of

materials to review in a limited timeframe, most entities focused their time reviewing the requirements, measures and VSLs. We have provided very few comments on the guidelines and technical basis sections due to time constraints. In addition, some standards had little or no guidelines in draft 2. It will take SDT resource time to get guidelines written for these standards for draft 3. We suggest considering separating the guidelines from the ballot process for standards for draft 3, to allow the drafting team to focus its efforts on making changes to the requirements, measures and VSLs to ensure approval of draft 3. The guidelines then can be finished on a separate timeline under the process in the NERC Standards Process Manual. It appears the manual provides a separate, quicker process for approving supporting documents like guidelines. (3) TABLE HEADERS: Change the column heading “Applicable BES Cyber Systems and associated Cyber Assets” to “Applicability.” The longer heading is confusing when there are no associated Cyber Assets listed in the column. (4) CAPITALIZATION WITHIN TABLE APPLICABILITY: Only words that are to be defined in the NERC glossary should be capitalized within the applicability column of the tables. For example, High Impact BES Cyber Systems should be changed to high impact BES Cyber Systems. (5) REFERENCES TO BES CYBER ASSETS/SYSTEMS: Throughout the requirements, rationales and guidelines, there are references to BES Cyber Assets and BES Cyber Systems, which are sometimes contradictory to the applicabilities. To eliminate this confusion, requirement text, rationales and guidelines should not include applicability. Rely on information in the applicability column to provide specific information on what assets are covered by the requirement. See especially CIP-004, -005, -007, -009, -010, -011. (6) MEASURES: Use the term “Examples” to introduce each of the measures. This would replace the standard language of “may include….but not limited to.” Auditors may interpret the current wording to mean that every item listed is required. In addition, verify that any measure that uses “and” instead of “or” is meant to require each of the items listed in the measures and format accordingly per the established convention for bullets vs. numbers. (7) ATTESTATIONS: There seems to be confusion within the industry regarding the use of attestations and when they are acceptable. Some of the measures in version 5 specifically list attestations. Does this preclude the use of attestations just because they are not specifically mentioned within the measures? (8) RECORDS RETENTION: Some requirements in V4 are for records retention, such as 90 days or 3 years. Draft 2 V5 appears to have a universal 3 year retention requirement in each standard under C. Compliance 1.2 Evidence Retention. Additionally, some V5 has some requirements for different retention periods. Is a requirement for evidence retention a “result” in the spirit of results based standards? Consider removing evidence retention requirements and incorporate them in the C. Compliance section with reference to their specific R and unique retention period, for example, 90 days. (9) A. INTRODUCTION 4. APPLICABILITY 4.2.3: Commenters have questioned if 4.2.3 should be removed because it may inadvertently create an exclusion for some control centers for entities that do not have BES Facilities. (10) Associated Protected Cyber Assets: These are listed in applicability throughout the requirements in all standards. Taken literally, for many requirements, it could be read to mean that while the control can be executed at a “System” level for highs, mediums, PACs and EACs, the control would have to be done on every Protected Cyber Asset. The Protected Cyber Assets should be covered as part of applying the control to their associated system. This is not clear in draft two. A possible solution is to revise applicability to, for example, “high impact BES Cyber Systems, including their associated Protected Cyber Assets.” In this way, the Protecteds are included in applying the control to the high.
Individual
Bob Thomas
Illinois Municipal Electric Agency
No
No
Yes
No
No
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
No
No
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.

Illinois Municipal Electric Agency supports comments submitted by American Public Power Association and Florida Municipal Power Agency.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Yes
Illinois Municipal Electric Agency supports comments submitted by American Public Power Association.
Illinois Municipal Electric Agency supports comments submitted by Florida Municipal Power Agency.
Individual
Richard Salgo
NV Energy
Yes
No
Yes
Yes
Yes
No
Yes
Control Center as it applies to the function of a Generation Operator has a threshold of generation located at two or more locations. This single qualifier could unintentionally sweep in the control centers for multi-location generation of very small capacity. We suggest that a capacity qualifier be added to this definition.
Connectivity: this definition begins with “A BES Cyber System that…” The noun in the defined term, Connectivity, cannot be defined as a “BES Cyber System”. We suggest the following re-write for the beginning of the definition: “External Routable Connectivity - The ability for a BES Cyber System to be accessible from a Cyber Asset…”
Yes
Group
Madison Gas and Electric Company
Joseph DePoorter
No
No
No
No
No
No

No
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Please see the MRO NSRF Comments.
Group
MRO NSRF
WILL SMITH
No
Yes
No
No
No
No
Yes
[A]The comments submitted by the MRO NSRF should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. [1]The NSRF comments on these definitions are predicated by our position that CIP-002-5 is fundamentally flawed, and the proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. More specifically, the impact rating should align with the facility instead of the cyber asset. Based on this position, the NSRF proposes the following changes to the definitions of “BES Cyber Asset” and “BES Cyber System”. [Proposed Verbiage] “BES Cyber Asset” should be defined as: “A Cyber Asset that if rendered unavailable, degraded, or misused would prevent one or more BES Sites from performing its reliability function for the Bulk Electric System. Redundancy of affected BES Sites and BES Cyber Assets shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)”. [Proposed Verbiage] The definition of “BES Cyber System” may then by modified as: “One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks at a BES Site for a functional entity.” [Clarification] NSRF requests clarification regarding demonstrating compliance for a BES Cyber System when not every device within the system can meet the requirement applied to the system, as a whole. We recommend that the system be not be found in a state of “non-compliant” as long as one or more devices within the identified system can fully meet the documented requirement and as long as every device within the system is documented as to its capability for meeting that requirement. If this is not the intent of the SDT, this issue must be addressed along with the definitions, because it is at this fundamental level that the Standards may or may not be applicable. [2] NSRF recommends the addition of a definition for a “BES Site” to be described as: “A registered entity-owned geographic location that: (1) performs the functional obligations of the Reliability Coordinator, Balancing Authority, Generator Operator, Generator Owner, Interchange Coordinator, Reliability Coordinator, Transmission Operator, or Transmission Owner, including Control Centers, Backup Control Centers and associated data centers that support those functional obligations, and(2) contains UFLS or UVLS Systems that are part of a

Load shedding program and Load-Serving Entity functional obligation, or(3) provides the protection or restoration of the BES while performing the functional obligations of Distribution Provider, or (4) provides Blackstart Resources, (and) that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact the reliability of the BES.”

NONE

[Proposed Verbiage] BES Cyber System Information: Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System, as defined within the Entity’s information protection program. Examples of BES Cyber System Information may include, but are not limited to, entity-specific security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses or security configuration information without context, ESP names, or policy statements. (Rationale: Removed the indication that the information had to be developed by the entity but still allowed for the omission of publicly-available vendor information in the program’s protection. Removed redundancy for “allowing unauthorized access”. Added security configuration information to the list of information without context that should not need special protection.E.g. generic hardening procedures.) [Proposed Verbiage] CIP Senior Manager: One management official with overall accountability and responsibility for the implementation of the entity’s NERC CIP program. (Rationale: removed “senior” to avoid implication that the official needs to be of a certain “rank” within the organization. Removed leading and added accountability phrasing to more accurately reflect the actual role within the organization.) [Proposed Verbiage] CIP Exceptional Circumstance: A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident that may require emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of workforce availability. (Rationale: removed “large scale” from the phrase regarding workforce availability. Workforce limitations may be localized or involve small numbers of personnel but may impact operations significantly. Added “that may” in front of ‘require emergency assistance’ to allow the entity to define the appropriate response on a case by case basis.)

NSRF appreciates the modifications made by the SDT to the standard and definitions related to physical security. [Proposed Verbiage] Physical Access Control Systems: Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. (Rationale: In order to remove the ambiguity around whether or not workstations used only for monitoring physical security alarms are subject to CIP requirements (e.g. guard’s desk), the word “alert” has been removed. The inclusion of “control” and “log” still ensure that the equipment that requires protection is included in the definition.)

[A] The comments submitted by the MRO NSRF should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. The definition of Electronic Access Control or Monitoring Systems is still too vague. For Access Control, specifically, does this mean every cyber system that might contribute to the authentication, authorization, and accounting (“AAA”) of a person crossing an EAP? If an entity uses Windows Active Directory for firewall authentication, for instance, this could be interpreted to mean every domain controller in the company is in scope. Extending that argument, the Help Desk PC that is used to grant access to the Windows Active Directory could be interpreted as being part of the AAA process, and therefore is itself an Electronic Access Control cyber asset. Likewise, a PC used at the guard desk (or third-party managed security provider) that is used to monitor alerts from the EAP could be considered a Cyber Asset used for Monitoring. Recommend the SDT provide a comprehensive list of cyber asset examples or “bright-line” set of criteria for Electronic Access Control or Monitoring Systems. [Proposed Verbiage] Electronic Access Control or Monitoring Systems: Cyber Assets that perform electronic access control or electronic access monitoring for Interactive Remote Access to the Electronic Security Perimeter(s) or Cyber Assets that perform electronic access control

or electronic access monitoring for Interactive Remote Access to BES Cyber Systems. Secondly, the NSRF would like to request that the SDT define the term “Access” used here and throughout the CIP standards, especially as it relates to cyber systems, or, specifically state that an entity can make their own definition of access such that different treatment can be given to high-risk access versus low-risk access. (“High-risk” meaning the ability to interact with, operate, modify, or cause availability issues with a BES Cyber System). Specific examples where “access”, if left undefined, could cause problems for an entity are: VMWare hypervisors, Oracle database clusters, or NAS systems that contain both BES and non-BES data/systems. Is the entity required to give CIP-004 treatment, for example, to an accounting clerk who has “access” to a receivables data table on an Oracle cluster that also hosts the backend database to a (BES) load control or EMS system? Does access to SCADA data, or a BES Energy Management System that also operates Distribution count?
[A]The comments submitted by the MRO NSRF should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. Does the definition of ESP presume the presence of an Electronic Access Point? In other words, does a BES Cyber System with no External Routable Connectivity fall within the scope of the CIP standards?Clarifying this point will pre-empt the need for interpretation or a CAN later. [Proposed Verbiage] Electronic Security Perimeter (“ESP”): A network to which BES Cyber Systems are connected using a routable protocol, surrounded by a logical border and which are only remotely accessible through an Electronic Access Point(s).
NONE
No
[1]In section 5 under “Initial Performance of Certain Periodic Requirements”, requirement CIP-010-5 R3, Part 3.2 is listed as needing to be initially performed within the first 12 calendar months. We request that this be pushed to at least 24 months to enable registered entities to perform two annual vulnerability assessments before attempting an active VA. Secondly, if industry approves the implementation requirements for planned and unplanned changes as being consistently 12 months, please collapse this section and simply state as such. The Disaster Recovery guidance is confusing, it seems to say “don’t hold up restoration for the sake of compliance, just be sure you’re in compliance at the end of restoration”, which seems to conflict. Please redraft to make it more clear what this intent of this section is. [2]The period between Version 4 and Version 5 enforceability needs to be addressed as it relates to Sites or Cyber Assets potentially requiring more protection in Version 4 than in Version 5. A transition period or a way to replace Version 4 with Version 5 protections must be allowed.
NONE
Group
Dominion
Connie Lowe
Yes
Yes
No
Yes
Yes
Yes
Yes
- The definition of BES Cyber Security Information is more clear if the last sentence is moved in front of the examples. The recommended definition is as follows, " Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by

themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures developed by the responsible entity and security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System. " - CIP Exceptional Circumstances: The definition should not be a prescriptive list and should allow each entity to define additional items as deemed appropriate. The recommended language for the definition is, " A situation that impact safety or BES reliability. Examples may include a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability."
Yes
GENERAL COMMENTS - 4.2.4 in the Applicability Section of all Standards states "Exceptions: The following are exempt from Standard CIP-002-5" as boiler plate language. The language contained in 4.2.4 needs to be updated to reference the the Standard within which the Applicability Section resides. For instance, 4.2.4 of the Applicability Section of CIP-003-5 states, "Exemptions: The following are exempt from Standard CIP-002-5" and should state, "Exemptions: The following are exempt from Standard CIP-003-5" - It should not be possible for Application Guidelines to change separately from the Standards themselves in such a way that the revised Application Guidelines would materially alter the interpretation of the requirement or add a "hidden" requirement not published in the Standard. - Where terms are defined in the glossary of terms, there is no need to duplicate the definition in the standards. An example of this is BES Cyber Asset where the definition is replicated in CIP-002. This definition should be removed from CIP-002 - The "not limited to" clause in the Measures section could be construed as "must have" evidence requirements. Where the clause exists, the starting phrase of the measure should be " Examples of acceptable evidence include..." along with a bulleted list. - CIP Exceptional Circumstances are only mentioned in CIP-004 and CIP-007. Since the timing of a CIP Exceptional Circumstance can't be predicted, CIP Exceptional Circumstances should be able to be applied to the overwhelming majority of the CIP Standards with few exceptions. Due to the lack of a "CIP Exceptional Circumstance" clause in most of the requirements, it appears as though strict compliance to the standards must be kept with little relief during these events. The ability to declare a "CIP Exceptional Circumstance" when appropriate and temporarily suspend strict compliance when it's in the best interest of the safety of personnel or the restoration or reliability of the Bulk Electric System is a critical concept that must be incorporated to guarantee the adoption of the CIP Standards. All requirements which result in the development of policies and procedures should not be subject to CIP Exceptional Circumstances, examples include CIP-002 (all), CIP-003 (all), and CIP-004 R2. Requirements that are expected to be executed during normal operations or under a defined periodic frequency should be able to be suspended where deemed appropriate upon a CIP Exceptional Circumstance, examples include CIP-004 R1.1, R3.2, R6.5, R6.6, R7.x; CIP-006 R1.2, R1.3, R1.4, R1.6, R1.8, R3.1; CIP-007 R2.3, R4.2, R4.5, R5.6; CIP-010 R3.1, and CIP-011 R1.3 - Clarify in the standards that CIP Exceptional Circumstances do not require or necessitate filing TFEs. - Should an entity determine through the use of the bright-line criteria in CIP-002 that it doesn't have any High or Medium Impact Cyber Systems, general clarity should be provided in Standards CIP-004 through CIP-011 as to whether or not additional Policies and Procedures need to be developed to address Standards which do not apply. - Where "associated" systems are identified in the Applicability column, the systems to which they are associated must be identified. An example of this is " Associated Physical Access Control Systems" which would be clarified if restated as " Associated Physical Access Control Systems for High Impact BES Cyber Systems" - The term "BES Cyber Assets", when used in the Requirements column should be replaced with the term "applicable Cyber Assets" to ensure the

applicability of the requirement in the Requirements column is in sync with the applicable Cyber Systems in the Applicability column. - The Applicability column should be consistently labeled "Applicability" across all of the tables in the standards.
Group
Southern Company Services, Inc.
Antonio Grayson
Yes
Yes
No
No
Yes
Yes
Yes
(1) Southern believes that for the purposes of the CIP standards a definition is needed and the current definition is acceptable.
(1) On page 1 of the definitions, the reference of “but are not limited to” in the second sentence of the definition of BES Cyber System Information definition should be struck. The word “example” by definition means that the list is not intended to be all inclusive. (2) On page 2, in the definition of CIP Exceptional Circumstance, the list of examples provided should not be considered to be all inclusive. In addition to the proposed change in the text, this point needs to be brought forth in the guidance. Original Text: A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability. "Proposed Text:" A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: examples may include a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability".
1) The definition of Physical Access Control Systems needs to ensure electronic visitor log books are not captured under the definition, and needs to include the word “or” instead of “and” . Original Text: "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers". Proposed Text: "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, electronic visitor log books, or badge readers".
No
Regarding the implementation plan, CIP-009-5, R2.3 is not listed as a recurring periodic activity in the “Initial Performance of Certain Periodic Requirements” table and should be. A full 3 years is needed to conduct an operational exercise of each recovery plan refrerenced in CIP-009-5 R1. Additionally, in the implementation plan, all the requirements are not identified in the initial section.
Southern’s comments on the overall standards (CIP-002 to CIP-011) include: (1) Across all CIP standards, measures need to be examples, not “may include, but not limited to”. The provided measures are “examples” and should be listed as such without further qualification. We suggest beginning all measures with the phrase “Example measures may include…” Listing examples without

calling them examples and including the “may include, but not limited to” language creates unnecessary confusion and conflict during all compliance activities, and especially during compliance audits. While Southern is supportive of the drafting team’s intent, under the present language Registered Entities cannot know if the listed measures are necessary, sufficient, neither, or both. (2) Across all CIP standards, in general, the language “at least once each calendar year, not to exceed 15 calendar months” creates two problems. First, a responsible entity has to perform two checks, one for calendar year and one for 15 months. Second, in any given calendar year, a 4th quarter activity cannot roll forward a quarter, however, 1st, 2nd, and 3rd quarter activity can roll to the following quarter in the following year. Southern suggests in each standard and requirement, where applicable, replace the text, “at least once each calendar year, not to exceed 15 calendar months” with the following proposed language: “at least annually, not to exceed 15 calendar months”. Alternatively, consider the equivalent language of “at least once each calendar year or not to exceed 15 calendar months”. (3) Across all CIP standards, measures need to be bullet points, not numbered lists. Numbered lists imply that all list entries are required rather than being examples. (4) Across all CIP standards, the SDT should clarify applicability of the 4.2.4.3 exemption to include any system covered under a NRC security plan, even if on a voluntary basis. (5) Across all CIP standards, a clarification is needed in the Reliable Operation of the BES section, sentence 2 (found on Page 8 of CIP-002, but needs to be clarified in all CIP standards). Rationale: Reliability tasks in the functional model apply to functions not Functional Entities as found in section. Original Wording: "In order to identify them, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for functional entities in the NERC Functional Model". Proposed Wording: "In order to identify them, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for functions in the NERC Functional Model." (6) Across all CIP standards, the applicability of each requirement should be exclusively in the Applicability column. There are numerous requirements where different types of systems are listed in the applicability column, but the requirement statement itself says “BES Cyber Systems”
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
No
Yes
Yes
Yes
Yes
Yes
Yes
The Consideration of Comments for Transient Cyber Asset in the previous draft states “The SDT has also incorporated suggestions that the connections could be made not only to another Cyber Asset, but also to the network within the ESP.” However, “network” was omitted from the parenthetical exclusion for temporary assets in the definition of “BES Cyber Asset” in this draft. Please clarify whether the exclusion in the parentheses applies to a Cyber Asset that is connected to a network (for example, connected to a non-programmable device such as a layer 1 Ethernet hub.) We suggest changing “it is directly connected to a Cyber Asset within an ESP, or to a BES Cyber Asset” to “it is directly connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, OR TO A NETWORK within the ESP”.
MMWEC agrees with and supports the comments submitted by APPA.
Yes

MMWEC agrees with and supports the comments submitted by APPA.
MMWEC agrees with and supports the comments submitted by APPA.
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
No
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
Please give consideration to the following suggestion: BES Cyber Asset – Replace the text at the end of the first paragraph, “. . . would affect the reliable operation of the Bulk Electric System”, to use a more clearly defined NERC Glossary term, “. . . would have an Adverse Reliability impact on the Bulk Electric System.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
ATC endorses the EEI consensus comments ss submitted by EEI for Comment Form D.
Group
NESCOR/NESCO
Annabelle Lee
No
The implementation plan calls for CIPv5 to come into effect July 1, 2015 (which has been moved out 6 months from the version one draft). Given that CIPv5 has already been in the works for more than two years, it is not clear why the effective date is three years in the future.
For all places where a requirement states "at least once every calendar year thereafter, not to exceed 15 months…”, this means that if the activity is performed every 15 months, then it would have only been performed 4 times in 5 calendar years. This contradicts the "at least once every calendar year…" Similarly for “every 39 months…”. To ensure that aircraft receive annual inspections once a year, Federal Aviation Regulation (FAR) 91.409(a) requires that" no person may operate an aircraft unless, within the preceding 12 calendar months, it has had (1) an annual inspection in accordance with part 43" etc. This wording precludes attempts to extendthe word "annual" to mean longer than one year, and we suggest that similar wording could be used in the CIPs. For example, "an entity is out of compliance with requirement Rxxx unless, within the preceding 12 calendar months, it has performed X Y Z". As stated in the document, "…from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities." Redundancy is not an appropriate mitigation for all vulnerabilities, but it is a mitigation for some. NERC may want to consider revising the sentence and being more specific when redundancy is not appropriate. As stated in the Table of Compliance elements, "100 High and Medium Impact BES Cyber Assets/Systems." Why are cyber assets listed in

some VSLs and cyber systems listed in others? As stated, "The term Facility is defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.).” The term element is not defined nor related to cyber assets/systems. NERC may want to consider adding a definition for element. NERC may want to consider adding iteration/feedback loops to the use case CIP process flow diagram. There is no clear requirement that non-routable communications between two ESPs, such as between a substation and control center, be encrypted or have their integrity assured. Technical solutions exist to secure serial SCADA communications, both in the form of proprietary vendor products, as well as standards such as IEEE 1711 (developed from AGA12) and Secure DNP3. We suggest that all non-routable persistent communications links between ESPs be protected with strong encryption and integrity. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. The lack of commercially available perimeter security solutions for non-routable protocols, pointed out in the Application Guidelines for CIP-005-5, further emphasizes the need for cryptographic protection of serial links. NERC's Consideration of Comments does not address this comment. This comment directly addresses point 86 in FERC 18 CFR Part 40 approving CIP v4, which states "…we support the elimination of the blanket exemption for non-routable connected cyber systems…" Cyber assets associated with data networks and data communications links between discrete ESPs, rather than being exempt from CIP requirements, could be specifically included, and exempt only when all communications between those ESPs are encrypted and have their integrity assured. IPSec VPNs have been a mature technology for many years, as are SSL VPNs. Given that these technologies are widely used in other industries, and that devices implementing them are available in industrial- and substation-grade form factors, we recommend that all routable communications, not just remote access connections, be protected with strong encryption and integrity (message authentication), using encryption technologies such as site-to-site secure VPNs. Secure VPNs should not be confused with technologies such as MPLS and GRE that can segregate traffic, but do not encrypt, and are therefore only secure if every intermediate device in the traffic path is secure. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. If communications assets are exempt from the CIPs as the draft currently states and communications are not encrypted and integrity verified, then every radio, modem, hub, communications device, wire, and fiber can provide an attacker with access to and the ability to falsify critical control system communications. This particularly applies to most private WANs leased from communications service providers: if communications over private WANs are not encrypted, then compromise of the service provider via mis-configuration, vulnerabilities in equipment, or insider collusion by employees of the service provider, could lead to compromise of multiple utility communications networks. This particularly applies to communications across the public Internet. Fully addressing security of communications links may require more than just removal of the A 4.2.4.2 exception. This topic seems sufficiently important to merit its own CIP section covering appropriate requirements for end-to-end protection of communications (encryption, integrity verification, key management, etc.). It is not clear that Security Event Monitoring as called out in CIP 007 is required of all EAPs. NERC could consider security event monitoring be required of all EAPs, regardless of impact level. CIP 011 does not address how third parties (consultants, contractors, vendors, etc.) should handle BES Cyber System information. Where 3rd parties have persistent or ephemeral remote access to Cyber Assets, they have implicit access to BES Cyber Asset information. NERC could consider applying all information requirements of CIP 011 to any 3rd parties with such access.
Individual
Brian S. Millard
Tennessee Valley Authority
Yes
Yes
Yes
Yes
Yes

Yes
Definition is too broad and subjective.
External Routable Connectivity - Insert “OSI layer level” in front of accessible in definitions.
Yes
Individual
Kirit Shah
Ameren
No
Yes
No
No
No
Yes
Yes
(1) BES Cyber Assets - The phrase "affect the reliable operation of the BES" used in the definition of a BES Cyber Asset needs to be defined, because one can argue that everything "affects" the reliable operation of the BES. Note that the word "adverse impact" is used with impact of the cyber asset on the Facility, while in CIP-002, page 8, it is used with impact on reliable operation of the BES. Please provide a definition and consistency between definition and CIP-002-5 documents.
Cyber System Information – This definition is poorly worded and seems convoluted. Please revise it so entities understand the intent of the SDT. One suggestion is to strike "but are not limited to" and "but not limited to" in the definition.
(1) Physical Access Control Systems – Please put a comma after second ‘Physical Security Perimeter’ so the ‘such as’ is referencing Cyber Assets, not ‘locally mounted hardware or devices’.
(1) Intermediate Device – The definition of an Intermediate Device should be changed to "A Cyber Asset or Collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate Device must be terminated on an Electric Access Point or be external to the Electronic Security Perimeter".
Yes
(1) Initial Performance of Certain Periodic Requirements – CIP-010 R3.2 should be given 36 calendar months instead of 12 calendar months to match the requirement timeframe. (2) Proposed Effective Date for Version - Delete the final sentence on Page 2, Part 1, starting with “Notwithstanding any order to the contrary…” and footnote #1 that goes with it since CIP version 4 has now been approved.
(1) There needs to be definition of "Dial-up Connectivity" added to the definitions. We suggest the following wording "Connectivity to a BES Cyber Asset (or associated Protected Cyber Assets) which uses a Public Switched Telephone Network (PSTN) that requires a number to be dialed".
Group
Salt River Project

Sara McCoy
Yes
Yes
Yes
Yes
No
SRP suggests clarification on the SDT's definition of Intermediate Device. Is it referring to a proxy type of device or some type of authentication device prior to accessing a BES Cyber System or Protected Cyber Asset?
Yes
Yes
Group
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)
David Dockery
No
Yes
No
Yes
Yes
Yes
No
[BES Cyber Asset, Definitions, p 1 REPLACE: “, and is used for” WITH: “, and is only used for” RATIONALE: AECI agrees with other commenters on the need for this clarification.]
[BES Cyber System Information, Definitions, pp 1 & 2 REPLACE: “the BES Cyber System” WITH: “a BES Cyber System” (all instances) RATIONALE: An Entity could have more than one BES Cyber System, or Information related to another Entity’s BES Cyber System.]
[Cyber Security Incident, Bullet #1, Defintions, p 1 REPLACE: “the Electronic Security” WITH: “a BES Cyber System’s Electronic Security” RATIONALE: Exclude all incidents of Physical Security Perimeter or Electronic Security Perimeter tampering, where no BES Cyber Systems are being protected, from being necessarily included as evidence and with necessary proof of evaluation that they were in fact not BES Cyber System related incidents.]
No
[Page 2, Part 1, final sentence beginning with, “Notwithstanding any order to the contrary...” REMOVE: the entire sentence along with accompanying footnote #1, or reword effectively. RATIONALE: The FERC Order accepting CIPv4 specifically states that it will supersede CIPv3, so this

sentence and footnote is now misleading at best. ALTERNATIVE: Restate this sentence such that it does, if approved by FERC, do what is suggested.]
[Page 2, Part 1, final sentence beginning with, “Notwithstanding any order to the contrary…” REMOVE: the entire sentence along with accompanying footnote #1, or reword effectively. RATIONALE: The FERC Order accepting CIPv4 specifically states that it will supersede CIPv3, so this sentence and footnote is now misleading at best. ALTERNATIVE: Restate this sentence such that it does, if approved by FERC, do what is suggested.] (Sorry, did not anticipate the comment-box on Question 15 above, so this is duplicated)
Group
FirstEnergy
Doug Hohlbaugh
No
Yes
Yes
Yes
Yes
No
Yes
(1) BES Cyber Asset – This definition states a “A Cyber Asset that if rendered unavailable, degraded, or misused ...” and FE suggests that the word “misused” be dropped from the definition to bring consistency with the latter part of the definition. Additionally, the preceding terms “rendered unavailable” and “degraded” better illustrate the intended risk or compromise to a BES cyber asset that warrants consideration to BES reliability risk. (2) BES Cyber System – FE proposes the following definition for BES Cyber System – “One or more BES Cyber Assets logically grouped by a responsible entity and interconnected via a routable protocol to perform one or more reliability tasks for a functional entity.” Similar to the proposed change for External Routable Connectivity, the BES Cyber System definition should be based on the routable connectivity of BES Cyber Assets. Non-routable devices (such as serially-connected RTUs) should fall outside of the BES Cyber System -- since they do not communicate via a routable protocol.
(1) External Routable Connectivity – We propose the definition focus on the cyber asset being routable and be re-written to state “A BES Cyber Asset that communicates with a Cyber Asset that is outside its associated Electronic Security Perimeter via a bi-directional routable protocol connection.” The reason for this change is that by defining external routable connectivity with respect to the BES Cyber Asset, rather than the BES Cyber System -- we take non-routable devices out of scope, as they are today. As written, we believe that all generation and transmission RTUs, relays, and any other devices that are part of the EMS or GMS BES Cyber Systems could potentially be brought in-scope. This would significantly increase the scope of covered assets, without a commensurate increase in security or reliability to the BES. There is other language in the Version 5 standard that needs to change to reflect this modification. For example, all of the "applicability" tables are based on the high/medium/low BES Cyber Systems "with External Routable Connectivity or dial-up connectivity." The applicability of the CIP Standards should be based on the qualifying connectivity of the BES Cyber Asset -- not the qualifying connectivity of the BES Cyber System (since the latter would bring assets into scope -- like serially-connected RTUs -- that do not have such qualifying connectivity). (2) Electronic Security Perimeter (ESP) – Similarly we suggest that the ESP definition be revised to focus on cyber assets and read “The logical border surrounding a network to which BES Cyber Assets are connected using a routable protocol.”

FE supports the Implementation Plan as stated in draft 2. However, we ask that the drafting team clarify their reasons for extending the low impact implementation plan by an additional 12 months beyond the high/medium impact requirements. Our understanding is that the additional time allotted is to allow industry to focus explicitly on meeting the requirements of the high/medium assets since they pose the greater risk to the BES. We concur with this approach, however, we are concerned that the very reason of this phased in implementation plan – permitting focus on high/medium BES Cyber Systems - once initial implementation periods are over will be lost during industry's on-going effort to ensure reliable cyber asset security. It should be recognized that expanding the scope to include low impact assets may in fact reduce security, since it diverts the focus of technical and compliance resources off of the areas that most require it. Due to the large administrative overhead involved and the compliance risk that it creates, low impact cyber assets and cyber systems should be out-of-scope entirely. On the other hand, draft 2 of CIP V5 appears to have greatly reduced the obligations for low impact cyber, to the point that the only requirement is a “policy document” in CIP-003-5 R3 with no requirement for an inventory, list, or discrete identification of low impact BES Cyber Systems and no other low impact requirements found within the CIP V5 standards. Based on the additional one-year allotted in the implementation plan, it is unclear what may be within scope of an audit of low impact cyber beyond the policy document in CIP-003 R3. We ask the team to clarify their reasons for the one-year extension and further explain the intended measures for ensuring CIP-003 R3 is met. Please see FE Comment Form A, Question #10 for changes we believe are needed for the measure of CIP-003 R3.
FE appreciates the efforts of the CIP draft team and it’s recognized that many of our prior comments are now reflected in the draft 2 set of CIP V5. We appreciate the team accepting our and others proposal to eliminate the use of BES Reliability Operating Services and to retain some of the existing terminology such as Physical Security Perimeter. As reflected in our comments we remain concerned that the standards need to remain focused on routable connectivity risk exposure and we offer some definitional changes in this regard. However, at a minimum we believe it is critically important to limit many of the requirement applicability associated with Medium BES Cyber Systems to Medium BES Cyber with External Routable Connectivity. Our submitted comments provide specific feedback in this regard.
Group
Duke Energy
Greg Rowland
No
No
No
No
No
No
No
(1) BES Cyber Asset. The definition of BES Cyber Asset is convoluted and confusing. The order of the phrase in the first sentence, “its required operation, mis-operation, or non-operation” needs to be changed at a minimum – the “required” seems to apply to mis-operation as well as operation. The first sentence overall is too long and confusing. And the sentence on redundancy is inconsistent with the first sentence; the first sentence uses the phrase “adversely impact” with respect to the Cyber Asset and the phrase “affect the reliable operation of the BES” with respect to Facilities, Systems or equipment, but the second sentence uses the phrase “adverse impact” with respect to Facilities, Systems and equipment. Duke recommends the following replacement definition, “A Cyber Asset that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the need, activation or exercise of the compromised Facility, System, or equipment.”. (2) BES Cyber System. Duke suggests that the definition be reworded to “One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks identified for functions in the NERC Functional Model.” This clarifies how the NERC Functional Model should be used in the assessment.
(1) The definition of Control Center uses language inconsistent with the NERC Functional Model. Duke

suggests the following rewording, “One or more facilities hosting functional entities that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks of functions in the NERC Functional Model of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.”
(1) BES Cyber System Information. Duke does not agree with examples being included in a definition. Examples should be reserved for guidance only and the definition should be limited to only prescriptive measures. Duke recommends rewording this definition to “Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.”. (2) CIP Exceptional Circumstance. Duke, however, sees the list of events provided in this definition as prescriptive and necessary. However, Duke recommends that the beginning be reworded to, “A situation that includes, but is not limited to, one or more of the following conditions that impact safety…”. Duke believes that this wording change adds flexibility to the entity to expand the definition to other events not listed, but at a minimum to consider those listed.
(1) Physical Access Control Systems. Duke does not agree with examples being included in a definition. Examples should be reserved for guidance only and the definition should be limited to only prescriptive measures. The exclusion of “devices at the Physical Security Perimeter” is also confusing. Could this inappropriately be interpreted to mean micros used for physical access control?
(1) Interactive Remote Access. Duke recommends that the following sentence, “Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants.” be removed. This section attempts to cover all methods of remote access, and appears to cover all types, but in the case that it doesn’t, the definition shouldn’t be limiting to just these scenarios. It is Duke’s opinion that the presentation of these scenarios is unnecessary. (2) Intermediate Device. Duke is concerned with the phrase “performing access control” existing as part of the definition of an Intermediate Device. Is it the drafting team’s intent that an Intermediate Device is also meeting the definition of an Electronic Access Control or Monitoring System? If so, Duke thinks that should be clarified in the definition of an Intermediate Device by saying that it is a specific class of EACMS devices. If it wasn’t the intent, distinction should be drawn between the two definitions.
(1) External Routable Connectivity. Duke would like to request that the drafting team consider using technical terms, such as the inclusion of network layers, to clarify what is meant by “accessible…via a bi-directional routable protocol”. Using network layers to quantify exactly the types of connections that are considered “externally routable” will aid in the entity’s assessment of this criteria. (2) Protected Cyber Asset. Duke would suggest removing the parentheses from the definition. Duke does not understand their purpose here.
(1) Reportable Cyber Security Incident. Duke suggests the following rewording of the definition to, “Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks identified for functions in the NERC Functional Model.” This clarifies the appropriate references back to the NERC Functional Model.
No
(1) Proposed Effective Date for Version 5 CIP Cyber Security Standards. The first sentence states that “Responsible entities shall comply with all requirements…”. This is in direct conflict with the next section titled “Initial Performance of Certain Periodic Requirements” which allows for some of the requirements to be initially compliant with after the initial effective date. Duke recommends replacing the word “all” with “the requirements in CIP-002, CIP-003…except for those listed below in the Initial Performance of Certain Periodic Requirements section”. (2) Proposed Effective Date for Version 5 CIP Cyber Security Standards. In the first listed item there is a reference to the fact that, “Notwithstanding any order to the contrary…”. Duke suggests that this language be removed. Duke sees this as unnecessary as FERC is able to approve/reject any or all of the Implementation Plan regardless of the language that is put in. Duke sees this type of language as unnecessary. (3) Unplanned Changes Resulting in a Higher Categorization. Duke has a concern that in the attempt by the drafting team to clarify the difference between a planned change and an unplanned change, a lot of unfair assumptions are made. For example, unplanned changes don’t account for a vertically-integrated utility. Does an entity have to talk to another entity that shares the same ownership for evaluation of a “planned” change? The examples provided cannot possibly address all scenarios and it

leaves the entities in a state of uncertainty as to which change the fall into. Duke suggests a simplification of addressing the addition of new Cyber Systems, reclassified Cyber Systems, etc. Duke requests that all scenarios of new or reclassified Cyber Assets that are intended to fall into the Implementation Plan have a single time window to meet compliance. Duke suggests that a 12-month implementation plan be used after the effective date of the change has been made. Duke also suggests that this section of the Implementation Plan cover the addition of EACMs, PACs, Protected Cyber Assets, and Low Impact BES Cyber Systems. Finally, Duke suggests that the 12-month implementation window be used for some of the requirements, but those identified in the “Initial Performance of Certain Periodic Requirements” be used for this section as well.
Group
Family Of Companies (FOC) including OPC, GTC & GSOC
Guy Andrews
Yes
Yes
Yes
Yes
No
see comments question 12
Yes
No
(BES Cyber Asset) Recommend modifying the parenthetical phrase. It is currently difficult to understand. We recommend the following modification: "A Cyber Asset is not a BES Cyber Asset if it is directly connected to a Cyber Asset within an ESP, including BES Cyber Assets, for 30 consecutive calendar days or less, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
none
none
none
We recommend adding the words “owned by or under the control of the Responsible Entity” to prevent the inclusion of equipment owned by Managed Security Providers in the standards. (Intermediate Device) The Devices involved in access control have been interpreted to include an entity's AAA servers; applying this interpretation to the proposed definition of Intermediate Device contains a requirement, which is not appropriate: “The Intermediate Device must not be located inside the Electronic Security Perimeter.”would prohibit an entity from protecting its AAA server(s) within an ESP. Consider rewriting the definition as follows: "A Cyber Asset or collection of Cyber Assets located on, or outside of the Electronic Security Perimeter that performs access control to restrict Interactive Remote Access to only authorized users". To qualify as an Intermediate Device, the asset(s) that actually restrict access must be located outside or on the ESP; devices that do not directly restrict access, but perform related functions such as authentication, authorization and logging may reside within the ESP." (Electronic Access Control and Monitoring Systems) We recommend adding the words “owned by or under the control of the Responsible Entity” to prevent the inclusion of equipment owned by Managed Security Providers in the standards.
(Protected Cyber Asset) See comment regarding BES Cyber Asset.
We believe “was an attempt” should be changed to “had the potential”. To know whether something was an attempt an entity would have to determine the intent of the perpetrator, who is many times never identified. Also, why would we want to exclude accidents which had the potential to disrupt operations from the scope of the standards?
Yes
none
none
Group

Texas RE NERC Standards Review Subcommittee
Brenda Hampton
No
No
No
No
No
See NSRS comments on Question 12.
Yes
No
(1) A Cyber Asset is not necessarily programmable. Modify the definition of Cyber Asset to read: “A Cyber Asset may be a programmable device (e.g., EPROM, microprocessor, etc.) that uses any combination of hardware, firmware, software, and/or data to execute internally stored programs and algorithms, including numerous arithmetic or logic operations, without operator action. Solid state devices (e.g., electro-mechanical on/off devices, relays, hard-wired logic devices, circuit boards, etc.) that do not have firmware and/or software are not considered Cyber Assets.” (2) In the definition of BES Cyber Asset, the discussion of redundancy is confusing, at best. We suggest replacing “Redundancy of affected Facilities, Systems, and equipment shall not be considered when determining adverse impact.” with “The use of redundant Facilities, Systems, or equipment to improve reliability and availability cannot form the basis to exclude assets from being considered as BES Cyber Assets.”
Modify the definition of Control Center to read: “One or more facilities hosting BES Cyber Assets/Systems including operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations.”
(1) In the second sentence of BES Cyber System Information, please strike the qualifier “…developed by the responsible entity” or, modify it to say “…security procedures followed by the responsible entity and whose disclosure could be used to gain unauthorized access”. The justification being that smaller entities may have their entire program developed, implemented, and/or managed by third-parties. (2) Modify the definition of CIP Senior Manager to read: “A single senior management official with overall accountability and responsibility for the implementation of the entity’s NERC CIP program” so as not to imply that it is a required that this person “lead” the implementation. (3) Modify the definition of CIP Exceptional Circumstances to read: “A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.”
Modify the definition of Physical Access Control System to read: “Cyber Assets that control, detect, alarm, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Revise definition of Interactive Remote Access to read: “All user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol or dial-up. Remote access 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) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.” Also consider adding a paragraph in the guidance section on what qualifies as a remote access client/remote access technology.
(1) Consider providing examples in the definition for Electronic Access Point. (2) Consider providing examples in the definition for Electronic Security Perimeter. (3) In the definition of a Protected Cyber Asset, suggest removing the parenthesis but keep the wording as a separate sentence.
(1) The words “malicious” and “suspicious” are subject to interpretation. Based on this, modify the definition of Cyber Security Incident to read: “A malicious act or suspicious event, as determined by

the registered entity, that: (1) Compromises, or was a plausible attempt to compromise a BES Cyber System, and/or (2) Disrupts, or was a plausible attempt to disrupt, the operation of a BES Cyber System.” (2) Currently the definition for Reportable Cyber Security Incident includes a reference to a reliability task. This is not a defined term and can be interpreted in many ways. We suggest modifying the definition to read “Any Cyber Security Incident that has compromised or disrupted one or more reliability functions.”
Yes
In section 5 under “Initial Performance of Certain Periodic Requirements”, requirement CIP-010-5 R3, Part 3.2 is listed as needing to be initially performed within the first 12 calendar months. We request that this be pushed to at least 24 months to enable registered entities to perform two annual vulnerability assessments before attempting an active vulnerability assessment.
See Question 15 for comments on the Implementation Plan.
Members of the Texas RE NERC Standards Review Subcommittee want to express our appreciation for the hard work of the Project 2008-06 CIP V5 Standard Drafting Team in responding to prior industry comments. We agree with many of the changes made since the previous version posting and are pleased with the progress that the team has made thus far.
Individual
Brian J Murphy
NextEra Energy, Inc.
No
No
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
Group
National Rural Electric Cooperative Association (NRECA)
Barry Lawson
No
No
Control Center – NRECA is concerned that in this definition the mere presence of a SCADA HMI might be considered a Control Center by a CEA if it could possibly be used to control BES assets in real-time even if an entity does not use it that way. Some of the registered entities do not staff these control centers 24/7 and are unable to perform real time control after hours, or any other time that other duties take them 15 minutes away from the computer. In some instances these entities might be registered as TOPs only because they own a limited and discrete 115 kV facility that no other entity

was willing to register as a TOP for. Often times this 115 kV facility performs no reliability function. NRECA suggests adding “24/7" to the first sentence of the Control Center definition as shown in the following text: “One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …”
CIP Senior Manager – In this definition replace “CIP Standards” with "CIP-002 through CIP-011." If this is not completed, this definition would apply to CIP-001 which still exists and is an unrelated standard. NRECA believes this revision will provide clarity to the limit of the definition.
Group
Florida Municipal Power Agency
Frank Gaffney
No
No
Yes
No
No
No
No
The definition of BES Cyber Asset uses the term “Systems” which is defined in the NERC Glossary as including distribution, i.e., “A combination of generation, transmission, and distribution components”. Distribution is specifically excluded from the standards through the Federal Power Act, Section 215, at (a)(1) and (i)(1). FMPA suggests eliminating the term altogether since the more general “equipment” already covers everything not covered by the term “Facilities”.
The definition of Control Center is ambiguous with its use of the phrase “perform the reliability functional tasks of”. If a Distribution Provider has a communication link from its SCADA system to a TOPs Control Center that sends the TOP data concerning load at more than one location, is that performing a monitoring function of a TOP? We do not believe that is the intent of the SDT, but, the phrase could be interpreted in that way. We suggest changing the phrase to specify that a Control Center is that BES Cyber System for which the System Operator has a Human Machine Interface.
The definition of Physical Security Perimeter is ambiguous as to whether it is two dimensional or three dimensional, and how such a perimeter might be different for High and Medium Impact systems. In other words, clarity as to the vertical dimension is needed, what size access “hole” needs to be controlled and is considered a physical access point (the 96 square inches in the guide is not enforceable, only requirements are enforceable), etc. Without such clarity, FMPA cannot vote Affirmative because entities will not know what is required and will likely have more surprises like CAN-0031 (which we believe is unenforceable).
The definition of Intermediate Device includes a requirement within it which should instead be included within the requirements of the standards, i.e.: “The Intermediate Device must not be located inside the Electronic Security Perimeter” should be deleted. The definition of Interactive Remote Access includes a sentence that adds no value, and does not address all circumstances: “Remote access may be initiated from …” should be deleted. It is possible to initiate remote access from assets owned by others not listed.
The definition of Protected Cyber Assets, which now excludes “transient devices”, which are considered cyber assets connected inside an ESP or attached to a Critical Asset for 30 days or less, we believe is too lenient on transient assets which can be used to “spread” Stuxnet type malware.

While we agree with treating transient devices differently than Protected Cyber Assets, we also believe there should be a requirement of a scan for malware on the transient device before it is connected to anything inside the boundary of the ESP for Medium and High Impact. FMPA believes that Transient Devices should be separately defined with an associated requirement within the standards.
The definition of a Cyber Security Incident includes an element that is not measurable as that term is used in the standards. It is essentially impossible to measure “an attempt to compromise” or “an attempt to disrupt”. This un-measurable definition will cause CIP-008-5 to be un-measurable. We suggest changing these terms to be measurable, e.g., attempts with known malicious intent such as discovered by malware protection.
Yes
COMMENTS ON APPICABILITY Under Applicability section 4.2.2, the phrase: “Distribution Provider: One or more of the Systems or programs designed, installed, and operated for the protection or restoration of the BES:” is ambiguous as to whether the following bullets is an exhaustive list (i.e.) or an “including but not limited to” list (e.g.). FMPA suggests clarifying that it is an exhaustive list by inserting “i.e.” at the end of the phrase. Under Applicability section 4.2.2, 3rd bullet, “A Protection System that applies to Transmission” is ambiguous. Instead, the term should be changed to “transmission Protection System” as used in PRC-004-2 and PRC-005-1 and for which there is a FERC approved interpretation (Project 2009 17). Under bullet 4.2.2, the term “required” is inappropriate for the 2nd and 3rd bullets, i.e., “… required by a NERC or Regional Reliability Standard”. Use of the word “required” implies an obligation to have evidence of why it is required. A more appropriate reference is “applicable”, e.g., “… applicable to a non-CIP NERC or Regional Reliability Standard” (the non-CIP is needed to prevent circular logic). Under bullet 4.2.2, the bullet on Cranking Paths needs to specify whose plan, i.e., “… in accordance with the applicable TOPs Restoration Plan.” COMMENTS ON COMPLIANCE ELEMENTS Measures are not enforceable and must not use the word “must”. On evidence retention, rather than restating the language of CMEP section 3.1.4.2, the evidence retention section of the standard should simply refer to that section of the CMEP so that if the ROP / CMEP is changed, the standards would not also need to be changed. As stated here, if the ROP/CMEP were to be changed, all the standards that repeat this language would also need to be changed with such change needing the approval of FERC, creating a lot of wasted effort and energy. FMPA understands that this section of the CMEP is currently being reviewed and evaluated for change. COMMENTS THAT APPLY TO SEVERAL DIFFERENT STANDARDS / REQUIREMENTS At least once a calendar year is sufficient, there is no reliability need for the “but not to exceed 15 calendar months” in any of the requirements that include that phrase. In reference to tables within the Requirements of nearly all of the standards, it is ambiguous as to whether the bullets are an exhaustive list (i.e.) or an “including but not limited to” list (e.g.). It is imperative that it be made clear that the list is an exhaustive list; otherwise the parent requirement can be interpreted as applying to all BES Cyber Systems, including Low Impact, when that is not the intent for many of the requirements. Change Management: there are several places in the standards where both: 1) an annual review is required, and 2) a requirement to change within 30 days of lessons learned or a change to systems/personnel. Both change management methods are not needed and the SDT ought to choose one method or the other to reduce administrative burden. This duplication of effort is made even worse with a third method of change management embedded within CIP-010-5, R3. TFEs: TFEs are an administrative nightmare with a very high administrative cost for little to no benefit to reliability. We recognize that the phrase “where technically feasible” is important because in some cases, it is not technically feasible. However, to reduce the administrative nightmare, it would be helpful to specify what would be required, if anything, if it were not technically feasible, so that a minimal amount of TFEs would need to be tracked. Such requirements would look like an “if” statement, e.g., if technical feasible to this, if not do that. In such a way, many TFEs could be eliminated.
Individual
Yuling Holden
PSEG
Yes
No

Yes
Yes
Yes
Yes
Yes
The definition of Control Center includes the undefined phrase “control of the Bulk Electric System (BES) in real-time to perform reliability functional tasks…” PSEG believes “control” must be clarified to ensure economic and market decision are not inadvertently captured by this definition. CIP-00-.5 (draft) page 23 of 33 includes a description of Monitoring and Control. The Control Center definition should capture the aspects of “control” in a manner consistent with what is included under Monitoring and Control (i.e. all methods of operating breakers and switches, SCADA, and substation automation). For CIP Exceptional Circumstance, even though the definition states “the following, or similar conditions,” we suggest changing “a natural disaster” to “a natural or human–caused disaster.”
Yes
Individual
Don Jones
Texas Reliability Entity
Yes
No
Yes
Yes
Yes
Yes
Yes
Individual
Daniel Duff
Liberty Electric Power LLC
No

No
No
Yes
Yes
Yes
Yes
Did not vote negative due to the definitions, but the definition of Cyber Asset suggests the reason the assets were grouped was for reliability. Would be better if the term was defined as a group of cyber assets used to enable functional interaction with or control of elements of the Bulk Electric System.
BES Cyber System Information needs to be clarified to exclude such items as the specific test formatting for relays and associated test results.
Yes
Group
Luminant
Rick Terrill
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
Individual
Stephanie Monzon
PJM Interconnection
Yes
No

Yes
Yes
Yes
Yes
Yes
Facility is unclear, definition would help with interpretation.
Yes
Individual
Kathleen Goodman
ISO New England Inc.
No
Yes
Yes
Yes
Yes
No
No
For clarity, suggest changing the BES Cyber Asset definition from "it is directly connected to a Cyber Asset within an ESP" to "it is directly connected to a network, or to a Cyber Asset within an ESP".
Request clarification on the definition of EAP. Must it be routable protocol on both sides?
The definition of Reportable Cyber Security uses the terms "compromised" and "disrupted" plus the phrase "reliability tasks of a functional entity". All three need their own definition/clarification.
No
Although the proposed Version 5 Implementation Plan states that “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan,” there are concerns that need clarification. The concerns refer to the transition from the currently effective Version 3, through Version 4 and finally to Version 5. Given that (a) the Version 4 Standards and associated Implementation Plan were recently approved by FERC; (b) the proposed Version 5 Implementation Plan contains a minimum 24-month period for enforcement means that there will be a period of time during which Version 4 would be effective; and (c) when Version 4 becomes effective there will be newly identified CAs that will have to be made compliant. In order to comply with Version 4 requirements, entities will be need to allocate funding and resources to perform work necessary to become compliant at newly identified

facilities. Much of this work must be performed in anticipation of the enforcement date. Once Version 5 becomes effective, application of the proposed categorization of BES Cyber Systems may very well result in much of the work done for Version 4 compliance being in the end unnecessary. Request clarification on the Disaster Recovery's "completion of the restoration activities" (top of the clean version's page 5). What event/action/etc. signifies this completion?
Section 5 for CIP-003-5 is the only place that explains how to read the bullets and numbers in the Measures. From the second paragraph of Section 5, "Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence." Request clarification this bullets and numbers explanations applies to the Requirements and Applicability sections of each of CIP-002-5 - CIP-011-1. If this was the SDT's intent, then recommend this clarification be added to Section 5 of each of CIP-002-5 - CIP-011-1. General comment--recommend that each Requirement’s Part identify that Part’s goal.
Group
Edison Electric Institute
David Batz
EEI REAC KEY ISSUES ISSUE 1: Low Impact BES Cyber Assets in scope (1.) FERC's version 4 Order 761 expects all BES Cyber assets should be in scope in V5. (2.) Audit issue of providing evidence of policy implementation on Low impact cyber assets. STRATEGY: Focus on 'BES site' level definition for Lows with security policy applied to sites, not individual cyber assets. ISSUE 2: Inclusion of Cyber Assets regardless of connectivity (1.) Blanket connectivity exclusion removed in CIP-002. Connectivity addressed in applicability column of requirements in CIP-003 to CIP-011. (2.) Example substation: Non-externally routable cyber assets increase cyber asset count 40% and some medium requirements are not good fits. STRATEGY: More liberal use of 'External Routable Connectivity' qualifier in the applicability column for more requirements throughout standards. ISSUE 3: Zero-defect requirements with compliance (not reliability) risk (1.) 8 of top 10 most violated standards in 2011. (2.) 91% of FFTs approved by FERC in March order which invited proposals to revise or remove requirements. (3.) NIST 800-53 App. E Minimum Assurance Requirements recognize flaws will be discovered and focus on continuous improvement. (4.) Other federal regulators do not enforce zero-defect perfection forever. STRATEGY: Overall NERC Standards issue and a philosophical change to requirements. Likely not to be fixed between drafts 2 and 3. Add language to the Requirement statement above the table for selected requirements. Language to incorporate the concepts of measuring performance to detect flaws, correcting flaws, taking action that may prevent recurrence (if applicable for the flaw) and flaws that have been detected and corrected are not violations. Reflect same concepts in the VSLs. ISSUE 4: Complexity of Applying the Requirements (1.) There are approximately 20 applicability references, so it's complicated to map the requirements to the classification of assets. (2.) However, this is the result of breaking up 'one size fits all' type requirements STRATEGY: The drafting team needs to produce a comprehensive mapping of each of classification of asset including all applicable requirements in a single document for and post it with Draft 3 to demonstrate how an entity would actually apply the requirements. Focus on sites for CIP-002 and Low and add requirements for medium and high per attachment 1. ISSUE 5: Blackstart units and cranking paths moved to Low Impact (1.) Concern that it is a lessening of V1-V4, FERC may remand STRATEGY: File as-is with technical and risk-based justification for not 'lessening' the standard. ISSUE 6: Immediate Revocation of access (1.) V5 requires that the revocation process be initiated immediately and completed within 24 hours. (2.) Though FERC Order 706 mandated 'immediate' revocation, many entities consider it

unattainable. STRATEGY: Limit to High Impact cyber assets only. Allow reasonable response time for Medium Impact and protected information. An example of unacceptable 'zero defect' risk, and a candidate for above strategy to add language in Requirement statement. ISSUE 7: Physical Access Controls for High Impact (1.) FERC Order 706 directed defense in depth ('two or more'). (2.) V5 limits this to control centers only. (3.) Many in the industry question if two different control systems are required. STRATEGY: Clarify in the Requirement that two authentication methods using the same control system are compliant (for example, badge/thumbprint). ISSUE 8: Violation Risk Factors (1.) One VRF is assigned to a requirement, regardless if it applies to both high and medium impact. STRATEGY: Where a medium VRF is proposed, revise it to medium for high impact and lower for medium impact. Change some mediums to lower. This may require double the number of requirements in order to have different VRFs for Highs and Mediums as NERC's format is rigid. ISSUE 9: Definition of Annual (1.) Annual is not in the NERC Glossary. V5 requires 'at least once every calendar year, but not to exceed 15 calendar months.' CAN-0010 establishes once per calendar year (unless the entity elects the tighter period of once within the last 12-month period). (2.) V5 is more restrictive than the NERC CAN. V5 creates a second criterion for reaching compliance in the 12 requirements where the above phrase is used. V5 creates a CIP-specific meaning of annual that is different from the other NERC standards. STRATEGY: Use 'annual' in V5. Alternatively, use 'once per calendar year or not to exceed 15 calendar months between occurrences.' This proposal is not more restrictive than CAN-0010. The proposal provides entities with more workload scheduling flexibility. ISSUE 10: Control Center Definition (1.) V5 creates a CIP-specific definition of 'Control Center.' CIP standards are not the only NERC standards using the term control center. (2.) The proposed CIP definition does not fit the context of the other NERC standards. Multiple definitions across reliability standards for the same term are confusing to implement and complicate auditing. (3.) The 300MW threshold in the proposed V5 definition has little basis relative to reliability. STRATEGY: Control Center should remain undefined in the CIP V5 standards and all references should be lower case. Create a separate project for team of experts in this area to devise a definition for the NERC Glossary of Terms. ISSUE 11: Physical Security Perimeter (PSP) Monitoring and Alerting (1.) V5 CIP-006 requires monitoring the PSP 24/7 for 'unauthorized circumvention of a physical access control into a PSP' and issuing an alarm 'in response to detected unauthorized circumvention of a physical access control into a PSP' in R1.4 and R1.5, respectively. (2.) V4 required monitoring and alerting of PSP access points. V5 eliminates the concept of access points and six-wall border. (3.) V5 can be read to mean monitoring and alerting of the entire PSP, not just the access points, such that video and/or motion detection would be needed for compliance. As such, V4 monitoring and alerting of access points for existing six-wall border PSPs may not be compliant for V5. STRATEGY: Clarify in the requirements R1.4 and R1.5 that if a six-wall border can be established then only the access points to a PSP need to have monitoring and alerting and not the entire PSP. If a six-wall border cannot be established then require monitoring and alerting for the entire PSP.
Individual
Andrew Gallo
City of Austin dba Austin Energy
No
No
No
No
No
Yes
No
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review

Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Yes
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Individual
Christina Conway
Oncor Electric Delivery Company LLC
Yes
Yes
Yes
Yes
No
INTERACTIVE REMOTE ACCESS COMMENTS: (1) Oncor has proposed that the definition of “Interactive Remote Access” or the applicability of CIP-005-5 R2 should be adjusted to reflect the exclusion of serially connected/non-routable/non-network connected devices. There is minimal reliability benefit and significant cost associated with applying the CIP-005-5 R2 requirements to all serially connected/non-routable/non-network connected devices that require remote access. Authentication when establishing connectivity to these systems is covered by CIP-005-5 R1.4 and provides the required cyber security. The cleanest way to correct this issue is to adjust the definition of “Interactive Remote Access” as follows: “All user-initiated access OF BES CYBER ASSETS WITHIN AN ELECTRONIC SECURITY PERIMETER 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 routable or dial-up access, using a client or remote access technology. Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.” Alternatively, the applicability of CIP-005-5 R2 could be changed from “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routable Connectivity.” (2) There is no mention of serially connected/non-routable/non-network connected devices in the CIP Awareness Bulletin (Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)) that initiated the CIP-005-3 SAR or the Guidance for Secure interactive Remote Access, which was ultimately issued after the CIP-005-3 revisions were not adopted. All discussions in these documents are in the context of IP addressable devices connected to a network that could be protected through the use of VPNs, proxy servers, etc. The current definition of “Electronic Security Perimeter” in the “Definitions of Terms Used in Version 5 CIP Cyber Security Standards” has evolved to make a delineation between devices that are connected to a network via routable protocol and those that are not. This further supports Oncor’s proposed adjustment to the definition of “Interactive Remote Access.” (3) In addition, in Consideration of Comments – Cyber Security Order 706 Version 5 CIP Standards (definition of “Electronic Access Point” section), it provides the following: “The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no ‘firewall’ capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs.” This demonstrates that the SDT considered and rejected the inclusion of serial, non-routable devices and specifically chose not to include them in the definition of “Electronic Access Point.” Thus, Oncor’s proposal is simply

urging that the same approach be taken with respect to “Interactive Remote Access” and that it should also not apply to serially connected/non-routable/non-network connected devices. (4) Oncor further requests additional information in the guidance section that addresses what is and is not a remote access client or remote access technology.
Yes
Yes
N/A
N/A
N/A
N/A
INTERACTIVE REMOTE ACCESS COMMENTS: (1) Oncor has proposed that the definition of “Interactive Remote Access” or the applicability of CIP-005-5 R2 should be adjusted to reflect the exclusion of serially connected/non-routable/non-network connected devices. There is minimal reliability benefit and significant cost associated with applying the CIP-005-5 R2 requirements to all serially connected/non-routable/non-network connected devices that require remote access. Authentication when establishing connectivity to these systems is covered by CIP-005-5 R1.4 and provides the required cyber security. The cleanest way to correct this issue is to adjust the definition of “Interactive Remote Access” as follows: “All user-initiated access OF BES CYBER ASSETS WITHIN AN ELECTRONIC SECURITY PERIMETER 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 routable or dial-up access, using a client or remote access technology. Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.” Alternatively, the applicability of CIP-005-5 R2 could be changed from “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routable Connectivity.” (2) There is no mention of serially connected/non-routable/non-network connected devices in the CIP Awareness Bulletin (Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)) that initiated the CIP-005-3 SAR or the Guidance for Secure interactive Remote Access, which was ultimately issued after the CIP-005-3 revisions were not adopted. All discussions in these documents are in the context of IP addressable devices connected to a network that could be protected through the use of VPNs, proxy servers, etc. The current definition of “Electronic Security Perimeter” in the “Definitions of Terms Used in Version 5 CIP Cyber Security Standards” has evolved to make a delineation between devices that are connected to a network via routable protocol and those that are not. This further supports Oncor’s proposed adjustment to the definition of “Interactive Remote Access.” (3) In addition, in Consideration of Comments – Cyber Security Order 706 Version 5 CIP Standards (definition of “Electronic Access Point” section), it provides the following: “The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no ‘firewall’ capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs.” This demonstrates that the SDT considered and rejected the inclusion of serial, non-routable devices and specifically chose not to include them in the definition of “Electronic Access Point.” Thus, Oncor’s proposal is simply urging that the same approach be taken with respect to “Interactive Remote Access” and that it should also not apply to serially connected/non-routable/non-network connected devices. (4) Oncor further requests additional information in the guidance section that addresses what is and is not a remote access client or remote access technology.
N/A
N/A
Yes
N/A
(1) In the comments that Oncor has submitted on Draft 2 Version 5 of the CIP Standards, there are

several instances in which Oncor has made specific suggestions for revised language that it was not able to provide in response to earlier draft versions. When Draft 2 Version 5 was made available, Oncor formed a team that performed an in-depth analysis of it from a broad cross-functional perspective. That team carefully analyzed each standard, the interactions of the standards, and how those standards could potentially impact reliability. This in-depth analysis led Oncor to the positions presented in its comments on Draft 2 Version 5. Oncor is committed to a successful ballot of CIP Version 5 and looks forward to the inclusion of these comments in Draft 3. (2) One of Oncor's primary concerns with Draft 2 of Version 5 of the CIP Standards is its broad application of many CIP requirements to cyber assets regardless of their connectivity, which results in an unreasonable expansion of the applicability of the CIP requirements to assets for which the additional requirements will provide minimal or no reliability benefit. Oncor urges the SDT to evaluate each draft standard and ensure that the protection each standard affords is applied in a reasonable manner. In its comments on each requirement in Draft 2, Oncor has identified those instances in which it believes that the applicability of the requirement has been expanded beyond what is reasonable and has provided language that identifies a more reasonable and appropriate applicability for that requirement. (3) Oncor also suggests the Standard Drafting Team develop a high level summary of the CIP Version 5 standards that shows the interaction between each standard, applicability type, and definition and provide that summary with the next draft. This will help eliminate any remaining inconsistencies and overlaps between standards prior to the next draft. (4) Oncor participated in the development of EEI consensus comments and supports the comments that EEI has submitted, as indicated in the individual question responses. (5) Oncor participated in the development of the Texas RE NERC Standards Review Subcommittee consensus comments and supports the comments that the Texas RE NERC Standards Review Subcommittee has submitted, as indicated in the individual question responses.
Individual
Scott Miller
MEAG Power
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Southern California Edison
Nathan Smith
Yes
No
Yes

Yes
Yes
SCE Comments to CIP-5 Definitions -Interactive Remote Access: Why is dial-up access considered here but not in all definitions? Please add the following definition: -Dial-up Access: Connectivity through 10-digit phone numbers dialed by a human using conventional public telephone lines.
No
Yes
-BES Cyber Asset: Although the definition is much improved it still does not prescribe how to document that an asset has been connected to the BES for less than 30 days. -CIP Senior Manager: Is the phrase "…overall authority and responsibility for…" intended to carry a different meaning from "…overall responsibility and authority for…" as it is written both ways in reference to the CIP Senior Manager?
-Control Center: What does the term "operating personnel" mean? We suggest revising this term to "BES operating personnel" or some other clarifying term.
-CIP Senior Manager: Is the phrase "…overall authority and responsibility for…" intended to carry a different meaning from "…overall responsibility and authority for…" as it is written both ways in reference to the CIP Senior Manager?
No comments
No comments
-Electronic Access Point: Please confirm the notion that cyber assets only communicate with other cyber assets?
No comments
No
SCE Comments to the CIP-5 Implementation Plan Initial Performance of Certain Periodic Requirements Section 5 provides a list of CIP Standards and Requirements that require compliance on a different schedule. Some standards require compliance as soon as within 14 days of the Effective Date of the Version 5 CIP Cyber Security Standards, however, the Proposed Effective Date for Version 5 CIP Cyber Security Standards Section provides for a 24 month implementation window. Please clarify that there is a minimum 24 month implementation window for all CIP Version Five standards.
Repeating, Initial Performance of Certain Periodic Requirements Section 5 provides a list of CIP Standards and Requirements that require compliance on a different schedule. Some standards require compliance as soon as within 14 days of the Effective Date of the Version 5 CIP Cyber Security Standards, however, the Proposed Effective Date for Version 5 CIP Cyber Security Standards Section provides for a 24 month implementation window. Please clarify that there is a minimum 24 month implementation window for all CIP Version Five standards.
-Protected Cyber Assets: The definition does not prescribe how to document that an asset has been connected to the BES for less than 30 days. Please add the following definition: -Dial-up Access: Connectivity through 10-digit phone numbers dialed by a human using conventional public telephone lines.
Individual
Heather Laws
POrtland General Electric
Yes
No
Yes
Yes
Yes
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary

to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI’s suggestions to strengthen the wording of this standard.
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI’s suggestions to strengthen the wording of this standard.
Individual
Don Schmit
Nebraska Public Power District
No
Yes
No
No
No
No
Yes
[A]The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. The NPPD comments on these definitions are predicated by our position that CIP-002-5 is fundamentally flawed, and the proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. More specifically, the impact rating should align with the facility instead of the cyber asset. Based on this position, the NPPD proposes the following changes to the definitions of “BES Cyber Asset” and “BES Cyber System”. “BES Cyber Asset” should be defined as: “A Cyber Asset that if rendered unavailable, degraded, or misused would prevent one or more BES Sites from performing its reliability function for the Bulk Electric System. Redundancy of affected BES Sites and BES Cyber Assets shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)”. The definition of “BES Cyber System” may then by modified as: “One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks at a BES Site for a functional entity.” NPPD recommends the addition of a definition for a “BES Site” to be described as: “A registered entity-owned geographic location that: (1) performs the functional obligations of the Reliability Coordinator, Balancing Authority, Generator Operator, Generator Owner, Interchange Coordinator, Reliability Coordinator, Transmission Operator, or Transmission Owner, including Control Centers, Backup Control Centers and associated data centers that support those functional obligations, and (2) contains UFLS or UVLS Systems that are part of a Load shedding program and Load-Serving Entity

functional obligation, or (3) provides the protection or restoration of the BES while performing the functional obligations of Distribution Provider, or (4) provides Blackstart Resources, (and) that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact the reliability of the BES.”
None.
[A]The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. [Proposed Verbiage] BES Cyber System Information: Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System, as defined within the Entity’s information protection program. Examples of BES Cyber System Information may include, but are not limited to, entity-specific security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses or security configuration information without context, ESP names, or policy statements. (Rationale: Removed the indication that the information had to be developed by the entity but still allowed for the omission of publicly-available vendor information in the program’s protection. Removed redundancy for “allowing unauthorized access.” Added security configuration information to the list of information without context that should not need special protection. E.g. generic hardening procedures.) [Proposed Verbiage] CIP Senior Manager: One management official with overall accountability and responsibility for the implementation of the entity’s NERC CIP program. (Rationale: removed “senior” to avoid implication that the official needs to be of a certain “rank” within the organization. Removed leading and added accountability phrasing to more accurately reflect the actual role within the organization.) [Proposed Verbiage] CIP Exceptional Circumstance: A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident that may require emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of workforce availability. (Rationale: removed “large scale” from the phrase regarding workforce availability. Workforce limitations may be localized or involve small numbers of personnel but may impact operations significantly. Added “that may” in front of ‘require emergency assistance’ to allow the entity to define the appropriate response on a case by case basis.)
[A] The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. NPPD appreciates the modifications made by the SDT to the standard and definitions related to physical security. [Proposed Verbiage] Physical Access Control Systems: Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. (Rationale: In order to remove the ambiguity around whether or not workstations used only for monitoring physical security alarms are subject to CIP requirements (e.g. guard’s desk), the word “alert” has been removed. The inclusion of “control” and “log” still ensure that the equipment that requires protection is included in the definition.)
[A] The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. The definition of Electronic Access Control or Monitoring Systems is still too vague. For Access Control, specifically, does this mean every cyber system that might contribute to the authentication, authorization, and accounting (“AAA”) of a person crossing an EAP? If an entity uses Windows Active Directory for firewall authentication, for instance, this could be interpreted to mean every domain controller in the company is in scope. Extending that argument, the Help Desk PC that is used to grant access to the Windows Active Directory could be interpreted as being part of the AAA

process, and therefore is itself an Electronic Access Control cyber asset. Likewise, a PC used at the guard desk (or third-party managed security provider) that is used to monitor alerts from the EAP could be considered a Cyber Asset used for Monitoring. Recommend the SDT provide a comprehensive list of cyber asset examples or “bright-line” set of criteria for Electronic Access Control or Monitoring Systems. [Proposed Verbiage] Electronic Access Control or Monitoring Systems: Cyber Assets that perform electronic access control or electronic access monitoring for Interactive Remote Access to the Electronic Security Perimeter(s) or Cyber Assets that perform electronic access control or electronic access monitoring for Interactive Remote Access to BES Cyber Systems. Secondly, the NPPD would like to request that the SDT define the term “Access” used here and throughout the CIP standards, especially as it relates to cyber systems, or, specifically state that an entity can make their own definition of access such that different treatment can be given to high-risk access versus low-risk access. (“High-risk” meaning the ability to interact with, operate, modify, or cause availability issues with a BES Cyber System). Specific examples where “access”, if left undefined, could cause problems for an entity are: VMWare hypervisors, Oracle database clusters, or NAS systems that contain both BES and non-BES data/systems. Is the entity required to give CIP-004 treatment, for example, to an accounting clerk who has “access” to a receivables data table on an Oracle cluster that also hosts the backend database to a (BES) load control or EMS system? Does access to SCADA data, or a BES Energy Management System that also operates Distribution count?
[A] The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. Does the definition of ESP presume the presence of an Electronic Access Point? In other words, does a BES Cyber System with no External Routable Connectivity fall within the scope of the CIP standards? Clarifying this point will pre-empt the need for interpretation or a CAN later. [Proposed Verbiage] Electronic Security Perimeter (“ESP”): A network to which BES Cyber Systems are connected using a routable protocol, surrounded by a logical border and which are only remotely accessible through an Electronic Access Point(s).
None.
No
[A] The comments submitted by NPPD should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. [1]In section 5 under “Initial Performance of Certain Periodic Requirements”, requirement CIP-010-5 R3, Part 3.2 is listed as needing to be initially performed within the first 12 calendar months. We request that this be pushed to at least 24 months to enable registered entities to perform two annual vulnerability assessments before attempting an active VA. Secondly, if industry approves the implementation requirements for planned and unplanned changes as being consistently 12 months, please collapse this section and simply state as such. The Disaster Recovery guidance is confusing, it seems to say “don’t hold up restoration for the sake of compliance, just be sure you’re in compliance at the end of restoration”, which seems to conflict. Please redraft to make it more clear what this intent of this section is. [2]The period between Version 4 and Version 5 enforceability needs to be addressed as it relates to Sites or Cyber Assets potentially requiring more protection in Version 4 than in Version 5. A transition period or a way to replace Version 4 with Version 5 protections must be allowed.
None.
Individual
Brian Evans-Mongeon
Utility Services Inc.
Yes
Yes
Yes
Yes

Yes
Yes
No
Utility Services supports the comments made by MMWEC in their Comments for BES Cyber Asset and BES Cyber System.
Please clarify the meaning of the word “locations”. Are properties that share the same BES point of interconnect considered to be one location? Suggest adding "and with two or more points of interconnection to the BES."
Utility Services suggest the removal of the word “single” from the CIP Senior Manager designation. “Official” is singular thereby making the word “single”, redundant.
None
None
None
None
Yes
None
None
None
Group
NCEMC
Scott Brame
Yes
No
No
Yes
Yes
Yes
Yes
NCEMC is concerned that in this definition the mere presence of a SCADA HMI might be considered a Control Center by a CEA if it could possibly be used to control BES assets in real-time even if an entity does not use it that way. Some of the registered entities do not man these control centers 24/7 and are unable to perform real time control after hours, or any other time that other duties take them 15 minutes away from the computer. In some instances these entities might be registered as TOPs only because they own a limited and discrete 115 kV facility that no other entity was willing to register as a TOP for. Often times this 115 kV facility performs no reliability function. NCEMC suggests adding “24/7 to the first sentence of the Control Center definition as shown in the underlined text: “One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time ...”
CIP Senior Manager – In this definition replace “CIP Standards” with CIP-002 through CIP-011. If this is not completed, this definition would apply to CIP-001 which still exists and is an unrelated standard. This revision will provide clarity to the limit of the definition.
Yes

Group
Dairyland Power Cooperative
Tommy Drea
No
Yes
No
No
No
Please see MRO NSRF comments.
No
Yes
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
No
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Please see MRO NSRF comments.
Individual
Jennifer White
Alliant Energy
No
Yes
No
No
No
No
Yes
Alliant Energy voted “No” on this list of definitions as we believe it is in fundamental conflict with the rest of the Standards. Proposed definitions herein should be considered within the context of the requirements, as well, due to considerable dependency between the proposed definitions and the proposed language changes throughout the rest of the Standards. Alliant Energy supports the MRO NSRF comments, as well. [1]Alliant Energy’s recommendations on these definitions are predicated by our position that CIP-002-5 is fundamentally flawed, and the proposed methodology prescribed by Requirement 1 is in direct conflict with the structure of the definition for BES Cyber Asset and BES Cyber System. More specifically, the impact rating should align with the facility instead of the cyber asset. Based on this position, Alliant Energy proposes the following changes to the definitions of “BES Cyber Asset” and “BES Cyber System”. [Proposed Verbiage] “BES Cyber Asset” should be defined as: “A Cyber Asset that within 15 minutes of being rendered unavailable, degraded, or misused would prevent one or more BES Sites from performing its reliability function for the Bulk Electric System. Redundancy of affected BES Sites and BES Cyber Assets shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)”. [Proposed Verbiage] The definition of “BES Cyber

System” may then by modified as: “One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks at a BES Site for a functional entity.” [Clarification] Alliant Energy requests clarification regarding demonstrating compliance for a BES Cyber System when not every device within the system can meet the requirement applied to the system, as a whole. We recommend that the system be not be found in a state of “non-compliant” as long as one or more devices within the identified system can fully meet the documented requirement and as long as every device within the system is documented as to its capability for meeting that requirement. If this is not the intent of the SDT, this issue must be addressed along with the definitions, because it is at this fundamental level that the Standards may or may not be applicable. [2] Alliant Energy recommends the addition of a definition for a “BES Site” to be described as: A registered entity-owned geographic location that: (1) performs the functional obligations of the Reliability Coordinator, Balancing Authority, Generator Operator, Generator Owner, Interchange Coordinator, Reliability Coordinator, Transmission Operator, or Transmission Owner, including Control Centers, Backup Control Centers and associated data centers that support those functional obligations, and(2) meets the criteria in CIP-002-5 Attachment 1 – Impact Rating Criteria Parts 3.1 – 3.5 and that (3) within 15 minutes of being rendered unavailable, degraded, or misused would prevent the entity from performing its reliability function for the Bulk Electric System.
[Proposed Verbiage] BES Cyber System Information: Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System, as defined within the Entity’s information protection program. Examples of BES Cyber System Information may include, but are not limited to, entity-specific security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses or security configuration information without context, ESP names, or policy statements. (Rationale: Removed the indication that the information had to be developed by the entity but still allowed for the omission of publicly-available vendor information in the program’s protection. Removed redundancy for “allowing unauthorized access”. Added security configuration information to the list of information without context that should not need special protection.E.g. generic hardening procedures.) [Proposed Verbiage] CIP Senior Manager: One management official with overall authority, accountability, and responsibility for the implementation of the entity’s NERC CIP program. (Rationale: removed “senior” to avoid implication that the official needs to be of a certain “rank” within the organization. Removed leading and added accountability phrasing to more accurately reflect the actual role within the organization.) [Proposed Verbiage] CIP Exceptional Circumstance: A situation that involves one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident that may require emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of workforce availability. (Rationale: removed “large scale” from the phrase regarding workforce availability. Workforce limitations may be localized or involve small numbers of personnel but may impact operations significantly. Added “that may” in front of ‘require emergency assistance’ to allow the entity to define the appropriate response on a case by case basis.)
Alliant Energy appreciates the modifications made by the SDT to the standard and definitions related to physical security. [Proposed Verbiage] Physical Access Control Systems: Cyber Assets that control or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers. (Rationale: In order to remove the ambiguity around whether or not workstations used only for monitoring physical security alarms are subject to CIP requirements (e.g. guard’s desk), the word “alert” has been removed. The inclusion of “control” and “log” still ensure that the equipment that requires protection is included in the definition. Also, the alerting requirement is still included in the Standards, so the protection will not be eliminated.)
[A] The comments submitted by the Alliant Energy should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead

of with the draft verbiage. Electronic Access Control and Monitoring Systems should be reduced to “Electronic Access Control Systems” and defined in the same structure as PACs. This is just for consistency and ease of use. If they perform the same functions, they should be parallel. Removed BES Cyber Systems to add clarity regarding the function of the EAP and the controls already required when External Routable Connectivity is at play. The definition of Electronic Access Control or Monitoring Systems is potentially still too vague. For Access Control, specifically, does this mean every cyber system that might contribute to the authentication, authorization, and accounting (“AAA”) of a person crossing an EAP? If an entity uses Windows Active Directory for firewall authentication, for instance, this could be interpreted to mean every domain controller in the company is in scope. Extending that argument, the Help Desk PC that is used to grant access to the Windows Active Directory could be interpreted as being part of the AAA process, and therefore is itself an Electronic Access Control cyber asset. Likewise, a PC used at the guard desk (or third-party managed security provider) that is used to monitor alerts from the EAP could be considered a Cyber Asset used for Monitoring. Recommend the SDT provide a comprehensive list of cyber asset examples or “bright-line” set of criteria for Electronic Access Control or Monitoring Systems. [Proposed Verbiage] Electronic Access Control or Monitoring Systems: "Cyber Assets that perform electronic access control or electronic access monitoring for Interactive Remote Access to the Electronic Security Perimeter(s).”
[A]The comments submitted by Alliant Energy should be considered collectively as they apply to the body of standards. If considered individually as they relate to specific standards or requirements, the intent of the comment, as well as its efficacy, will be difficult to judge. Each element of proposed verbiage should be considered along with proposed verbiage in other portions of the standard instead of with the draft verbiage. Does the definition of ESP presume the presence of an Electronic Access Point? In other words, does a BES Cyber System with no External Routable Connectivity fall within the scope of the CIP standards?Clarifying this point will pre-empt the need for interpretation or a CAN later. [Proposed Verbiage] Electronic Security Perimeter (“ESP”): A network to which BES Cyber Systems are connected using a routable protocol, surrounded by a logical border and which are only remotely accessible through an Electronic Access Point(s). [Proposed Verbiage] Protected Cyber Asset: “A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter (a Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes).” Removed “directly” to allow connection within the ESP without requiring the connection to be through a BES Cyber System or Cyber Asset.
[Proposed Verbiage] Remove “Any” from Reportable to be consistent with the change to Cyber Security Incident.
No
Alliant Energy voted “No” to the proposed implementation plan due to the comments herein. [1]In section 5 under “Initial Performance of Certain Periodic Requirements”, requirement CIP-010-5 R3, Part 3.2 is listed as needing to be initially performed within the first 12 calendar months. We request that this be pushed to at least 24 months to enable registered entities to perform two annual vulnerability assessments before attempting an active VA. Secondly, if industry approves the implementation requirements for planned and unplanned changes as being consistently 12 months, please collapse this section and simply state as such. The Disaster Recovery guidance is confusing, it seems to say “don’t hold up restoration for the sake of compliance, just be sure you’re in compliance at the end of restoration”, which seems to conflict. Please redraft to make it more clear what this intent of this section is. [2]The period between Version 4 and Version 5 enforceability needs to be addressed as it relates to Sites or Cyber Assets potentially requiring more protection in Version 4 than in Version 5. A transition period or a way to replace Version 4 with Version 5 protections must be allowed.
[VSL] Alliant Energy strongly recommends that the VSLs be revisited to address the zero tolerance approach. Additionally, they are structured such that there is no variance in severity based on the impact rating of the cyber system or the specific element of the sub-requirement. This needs to be addressed in order to ensure that the entities can be held accountable at the right level based on actual risk. [BES Cyber Systems and BES Cyber Assets] If the creation of the BES Cyber System was introduced with the intent to eliminate the need for TFEs, Alliant Energy agrees with the intention, but not the execution. The concept is not applied consistently throughout the Standards, insofar as there

are requirements that apply at the device level. Additionally, it is not clear how many of the BES Cyber Assets within a system must meet the requirement in order to avoid a finding of non-compliance for the system. Alliant Energy recommends returning to the Critical Cyber Asset terminology, as it allows entities to retain currently existing documentation if it is sufficient to meet the new Standards. Also, this terminology can be successfully used to implement programs while avoiding the TFE if the proposed recommendations related to the VSLs and the implementation of programs that recognize and mitigate for specific configuration. The Standards should be written such that the entity’s understanding of its own devices and vulnerabilities is required, not that device by device configuration constitutes a violation.
Individual
Nathan Mitchell
American Public Power Association
Yes
Yes
Yes
Yes
Yes
Yes
Yes
APPA agrees with the revised definition of Control Center. The SDT has focused the definition to the core of what a Control Center really is; real-time operations, hosting operating personnel, and perform the functions of RC, BA, TOP, or GOP. With this clear definition, many small entities will be spared the burden of proving that their distribution dispatch centers are not Control Centers. However, in the webinar conducted by the SDT a question was raised on the issue of “manual and voice instruction” as a “control” where this term is used in the definition. The SDT referred this question back to the CIP Version 1 FAQ from May 9, 2005 where it was stated: “monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction.” APPA has a real concern that the SDT has interpreted the term “control” in a way that will eliminate the option of removing/not installing “remote accessible or automatic controls” as a way to mitigate the risk of a cyber incident within a “monitor only” control center. This type of control center should not be required to implement the High or Medium Impact requirements in CIP-003-5 through CIP-011-5 nor document compliance with these standards. APPA believes that having an intelligent operator as the device between the monitored cyber asset and the actual “manual or voice instruction control” is “air gapped.” APPA believes that a control center built without remote accessible or automatic controls should be designated as a Low Impact facility. This designation will help reduce the burden of compliance for small entities that chose to use this cyber risk mitigation method. APPA Recommendation: Clarify in guidance what “control” within the Control Center definition means. If the SDT uses the CIP Version 1 FAQ response as the guidance: “monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction” APPA recommends that control centers which use only manual or voice instruction as the control be designated as Low Impact facilities in CIP-002-5 Attachment 1.
Yes
APPA agrees with the revision of the implementation timeframe. Having a High and Medium Impact implementation timeframe set at 24 months or July 1, 2015 will focus the industry on developing compliance documentation for these critical facilities first. This may work well with the CIP Version 4 coordination as most of those facilities identified in Attachment 1 may already be identified and in the

process to be covered under a compliance plan. APPA agrees with the 36 month or July 1, 2016 implementation plan for Low Impact facilities. This will give those entities setting up completely new CIP compliance programs enough time to budget and incorporate these plans prior to enforcement.
APPA has focused our comments on the impact of the standards on small entities. We recommend that the SDT take a close look at the applicability and the requirements in all of the CIP Version 5 standards. Where the standards are applicable to small entities the SDT needs to account for the impact on small entities and only include those requirements if they are absolutely critical for the protection of the reliability of the BES. If these requirements must be included, than the SDT should allow for a small entity exemption process.
Individual
Tracy Richardson
Springfield Utility Board
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
David R. Rivera
New York Power Authority
No
Yes
Yes
Yes
Yes
No
No
NYPA agrees with NPCC comments.
NYPA agrees with NPCC comments
NYPA agrees with NPCC comments
No

NYPA agrees with NPCC comments, plus - NYPA would like clarification regarding implementation time periods for disaster recovery (pg 4,5); there is an allowance to handle the emergency without worrying about compliance activities but then they want compliance to be met otherwise it’s a violation. What is the time frame to get the system compliant after the disaster recovery? Also, the section on “Initial performance of certain periodic requirements” should include CIP-009 R2 part 2.3 under item 5.
NYPA agrees with NPCC comments, plus - NYPA would like clarification regarding implementation time periods for disaster recovery (pg 4,5); there is an allowance to handle the emergency without worrying about compliance activities but then they want compliance to be met otherwise it’s a violation. What is the time frame to get the system compliant after the disaster recovery? Also, the section on “Initial performance of certain periodic requirements” should include CIP-009 R2 part 2.3 under item 5.
Group
Progress Energy
Jim Eckelkamp
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Progress Energy agrees with EEI comments with the modified and additonal comments below: Issue = Low Impact BES Cyber Assets in scope • FERC’s version 4 Order 761 expects all BES Cyber assets should be in scope in V5. • Audit issue of providing evidence of policy implementation on Low impact cyber assets. Strategy =Focus on ‘BES site’ level definition for Lows with security policy applied to sites, not individual cyber assets. Issue = Inclusion of Cyber Assets regardless of connectivity • Blanket connectivity exclusion removed in CIP-002. Connectivity addressed in applicability column of requirements in CIP-003 to CIP-011. • Example substation: Non-externally routable cyber assets increase cyber asset count 40% and some medium requirements are not good fits. Strategy = More liberal use of ‘External Routable Connectivity’ qualifier in the applicability column for more requirements throughout standards. Issue= Zero-defect requirements with compliance (not reliability) risk • 8 of top 10 most violated standards in 2011. • 91% of FFTs approved by FERC in March order which invited proposals to revise or remove requirements. • NIST 800-53 App. E Minimum Assurance Requirements recognize flaws will be discovered and focus on continuous improvement. • Other federal regulators do not enforce zero-defect perfection forever. Strategy= Overall NERC Standards issue and a philosophical change to requirements. Likely not to be fixed between drafts 2 and 3. Issue= Complexity of Applying the Requirements • There are approximately 20 applicability references, so it’s complicated to map the requirements to the classification of assets. • However, this is the result of breaking up ‘one size fits all’ type requirements Strategy= The drafting team needs to produce a comprehensive mapping of each of classification of asset including all applicable

requirements in a single document for and post it with Draft 3 to demonstrate how an entity would actually apply the requirements. Focus on sites for CIP-002 and Low and add requirements for medium and high per attachment 1. issue= Blackstart units and cranking paths moved to Low Impact • Concern that it is a lessening of V1-V4, FERC may remand Strategy= File as-is with technical and risk-based justification for not “lessening” the standard. Issue= Immediate Revocation of access • V5 requires that the revocation process be initiated immediately and completed within 24 hours. • Though FERC Order 706 mandated “immediate” revocation, many entities consider it unattainable. Strategy= Limit to High Impact cyber assets only. Allow reasonable response time for Medium Impact and protected information. An example of unacceptable “zero defect” risk, and a candidate for above strategy to add language in Requirement statement. Issue= Physical Access Controls for High Impact • FERC Order 706 directed defense in depth (“two or more”). • V5 limits this to control centers only. • Many in the industry question if two different control systems are required. Strategy= Clarify in the Requirement that two authentication methods using the same control system are compliant (for example, badge/thumbprint). Issue= Violation Risk Factors • One VRF is assigned to a requirement, regardless if it applies to both high and medium impact. Strategy= Where a medium VRF is proposed, revise it to medium for high impact and lower for medium impact. Change some mediums to lower. This may require double the number of requirements in order to have different VRF’s for Highs and Mediums as NERC’s format is rigid. Issue= Definition of Annual • Annual is not in the NERC Glossary. CAN-0010 establishes once per calendar year (unless the entity elects the tighter period of once within the last 12-month period). • V5 requires “at least once every calendar year, but not to exceed 15 calendar months”. • V5 is more restrictive than the NERC CAN and V5 creates a second criterion for reaching compliance in the 12 requirements where the above phrase is used. Strategy= Consider using “annual” in V5 and the use of “or”.
Individual
Maggy Powell
Exelon Corporation and its affiliates
No
No
No
No
No
No
Yes
BES Cyber Asset – support as proposed BES Cyber System – The use of the terms “responsible entity" and "functional entity" is inconsistent and confusing. It appears that the proposal is to define new terms to describe items that are covered by existing definitions. In other standard development projects we’ve seen similar attempts (i.e. NUC-001 and the definition of “Transmission Entity”) which resulted in added confusion. Defining new terms when existing terms suffice should be avoided. Our assumption is that the definition of Functional Entity refers to the term as defined in the Functional Model. It is critical to clarify that we are consistently using one definition, so please clarify whether the SDT intended to refer to this definition. Responsible Entity is not defined in the NERC Glossary of Terms or Functional Model; though, it is capitalized in the Applicability section (section 4) of the CIP version 5 standards. The term is not capitalized in the BES Cyber System definition. Is the responsible entity in the BES Cyber System definition intended to be the same as Responsible Entity in the Applicability? Further, the creation of a "responsible entity" may go beyond the boundary of a registered functional entity. Only a registered entity can be accountable to the standards even if that entity arranges/contracts for another party to conduct a function covered by a standard. To clarify and avoid a potential expansion of scope, consider the following revision: "BES Cyber System - One or more BES Cyber Assets logically grouped to perform one or more reliability tasks for a Functional Entity." Cyber Asset - Support as proposed
Control Center should not be defined as part of the CIP standards. The complexities around control centers warrant that a focused team work to define control center as part of a separate project. Further, other standards beyond CIP utilize the term “control center” and the context for those standards is relevant to the discussion in defining the term. If defined by the CIP standards, it will be

inappropriate to apply that definition to the same term in another standard. As well, multiple definitions across reliability standards will be confusing and complicates auditing. The project to define Bulk Electric System (BES) included the task to identify all locations and contexts in which the BES term appeared. In developing an appropriate definition, the analysis included this look at the term's role across all standards. Definition of Control Centers should be afforded the same analysis. Control Center should remain undefined in the CIP V5 standards and all references should be lower case. Specific to the proposed language, it is problematic that the definition is not aligned with reliability impact. Defining a control center by the number of associated locations is not indicative of the role to reliability that the particular control center may or may not play. While CIP-002 Attachment 1 attempts to delineate degree of impact through thresholds (i.e. 300 MW for Medium in 2.11) these thresholds are weakly aligned with reliability impact. For example, a single generating facility's control room could control 1000 MW at a single location and not be a control center, but another facility's control room could control 290 MW in the location in which it resides along with remote start capability for another facility's 90 MW unit and become a control center. The perverse incentive created is to disconnect remote connectivity which is contrary to reliable practice. We recognize the challenge in finding an appropriate threshold measure and struggle to offer an alternative. Thus, we prefer that a focused team tackle the matter. Inclusion of this definition is a primary reason for the NEGATIVE votes on CIP-002. While definitions cover the full suite of standards, we opted to reflect the definition's influence on voting in the CIP-002 ballot to enable our support for some standards. If the SDT insists on creating a control center definition, we suggest that the definition focus on applicability to the CIP standards by naming the definition "CIP Control Center." This will limit the impact on the use of control center in other standards, but still provide a model definition for the term. To clarify the definition language further, please consider the following revisions: A facility hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at three or more locations, or 4) a Generation Operator for generation Facilities at three or more locations.
BES Cyber System Information – support as proposed CIP Exceptional Circumstances – The definition appears to be too broad and as a result causes concerns with CIP-006 Parts 2.1 and 2.2 (and others). For example, under the proposed version of the definition CIP-006-5 Part 2.1 requires continuous escort of visitors except in a CIP Exceptional Circumstance. This case allows a blanket exception for all visitors within the PSP to avoid escort (including ones already inside under escort), which seems contrary to the intent of Part 2.1 (actual intent being things like emergency medical personnel). It seems appropriate to require continuous escort under the following conditions: civil unrest; imminent or existing hardware, software, or equipment failure; enactment of a mutual assistance agreement; and impediment of large scale workforce availability. To remedy this issue, we recommend that these situations and the words "or similar," be removed from the definition of CIP Exceptional Circumstance to read: CIP Exceptional Circumstance - A situation that involves one or more of the following conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, a Cyber Security Incident requiring emergency assistance, and a response by emergency services. CIP Senior Manager – support as proposed
Physical Access Control Systems – support as proposed Physical Security Perimeter – We appreciate the return to PSP. For consistency, the definition should read "Control or Monitoring". Proposed revision: Physical Security Perimeter – "The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled."
Electronic Access Control and Monitoring Systems – support as proposed Interactive Remote Access – The language is not clear as to what is to be accessed. To clarify, consider the following revision: Interactive Remote Access - All user-initiated access to a BES Cyber Asset by a person that originates from a Cyber Asset outside the Electronic Security Perimeter that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether routable or dial-up access, using a client or remote access technology. Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications. Intermediate Device – The term "device" raises concern. The term "device" is understood in practice as describing a broader set of assets than appropriate to apply in the CIP standards. In addition, it's not clear whether

software is considered a device even though we recognize that software runs on something that could be considered the device. To clarify, please consider replacing "Intermediate Device" with "Intermediate Cyber Asset".
Electronic Access Point – Some confusion remains about whether an EAP is part of the ESP or not. As we understand the intention is for an EAP is a point on the ESP. The example referenced is an EAP could be a port on a firewall, but not the firewall itself. The term “interface” is understood by some to be card or item inside the ESP rather than on the ESP as the definition seems to intend. Please consider removing the term “interface” so that the definition reads: Electronic Access Point (“EAP”) - A Cyber Asset on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter. Electronic Security Perimeter – support as proposed External Routable Connectivity – The current language defines "connectivity" as a system rather than a state in which the system finds itself. Consider the following revision: "External Routable Connectivity - The property of a BES Cyber System that is accessible from a Cyber Asset that is outside its associated Electronic Security Perimeter via a bi-directional routable protocol connection." Protected Cyber Asset – support as proposed
Cyber Security Incident – support as proposed Reportable Cyber Security Incident – support as proposed
No
While the revised Implementation Plan is an improvement, concerns remain. The sections on unplanned and planned changes are incomplete and the examples are contradictory. The proposed Implementation Plan clearly states that an unplanned change includes a generation plant modification changing its rated output. Typically, the entity that owns that generation site has to plan to change the output. The document states that planned changes are changes which were planned and implemented by the responsible entity. Where would an up-rate of a generation site reside - planned or unplanned? Further, the plan calls for one year (two years if first time) to comply with the suite of standards if it is an unplanned change. The comprehensive nature of the standards is independent of whether a change is planned or unplanned. There does not appear to be added reliability risk associated with planned changes, therefore, we propose that any change, planned or unplanned be given a year (two years if first time) to comply with the standards. We support the Previous Identity Verification language.
VSLs: VSLs do not cover scenario for failure to update documentation of BES Cyber Assets for more than 80 days but less than 90 days, i.e., moderate VSL covers 70 - 80 days and high VSL covers 90 - 100 calendar days. Please correct calendar ranges for moderate and high VSLs. It remains unclear how the numbers within the VSLs relate to reliability. Applicability: Similar to our concerns with the definition of BES Cyber System, the Applicability language appears to define new terms to describe items that are covered by existing definitions. In other standard development projects we’ve seen similar attempts (i.e. NUC-001 and the definition of “Transmission Entity”) which resulted in added confusion. Defining new terms when existing terms suffice should be avoided. Our assumption is that the definition of Functional Entity refers to the term as defined in the Functional Model. It is critical to clarify that we are consistently using one definition, so please clarify whether the SDT intended to refer to this definition. Responsible Entity is not defined in the NERC Glossary of Terms or Functional Model; though, it is capitalized in the Applicability section (section 4) of the CIP version 5 standards. It is not capitalized in other points in the standards. Further, the creation of a "responsible entity" definition may go beyond the boundary of a registered functional entity. Only a registered entity can be accountable to the standards even if that entity arranges/contracts for another party to conduct a function covered by a standard. Exemptions: We support the continued use of the language in 4.2.4.3 to reiterate the nuclear plant exemption, providing clarity in cyber security regulation of nuclear facilities. This exemption is consistent with the approved Version 4 Standards, the March 10, 2011 FERC Order (Docket# RM06-22-014) and the Memorandum of Understanding between NERC and the NRC (dated 12/30/2009).
Individual
Steve Karolek
Wiscsonsin Electric Power Company
No

Yes
Yes
Yes
No
No
Yes
Wisconsin Electric Power Company supports EEI Member Consensus comments as submitted by EE
In the definition of Interactive Remote Access, it is not necessary to discuss who owns a specific Cyber Asset from which it is initiated. The list provided does not appear to be inclusive enough. For example, what about a Cyber Asset owned by a hotel at which an employee or contractor is staying? What about a Cyber Asset owned by an "Internet Cafe" or a public library?
The definition of "External Routable Connectivity" needs to be reworded to clarify it is the ability to communicate with a BES Cyber System. The current wording says External Routable Connectivity "(is) A BES Cyber System..."
Yes
The term "Annual" should specifically added to the definitions as applied in NERC CAN-0010. This definition of Annual should be used throughout the standards in place of "each calendar year, not to exceed 15 months" since "calendar year" and "15 months" are incompatible measures. There are three months of the calendar year where a circumstance which causes an expected process to be executed longer than 12 months but less than 15 months since the previous execution would result in a violation of the "each calendar year" portion of the requirement.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
No
No
Yes
Yes
Yes
Yes
No
BES Cyber System, Control Center, and Reportable Cyber Security Incident: BES Cyber System and Reportable Cyber Security Incident definitions refer to “reliability tasks”; while the definition of Control Center refers to “reliability functional tasks of a RC, BA, TOP or GOP” the drafting team should clarify if these tasks are intended to be the same
BES Cyber System, Control Center, and Reportable Cyber Security Incident: BES Cyber System and Reportable Cyber Security Incident definitions refer to “reliability tasks”; while the definition of Control Center refers to “reliability functional tasks of a RC, BA, TOP or GOP” the drafting team should clarify if these tasks are intended to be the same

BES Cyber System, Control Center, and Reportable Cyber Security Incident: BES Cyber System and Reportable Cyber Security Incident definitions refer to “reliability tasks”; while the definition of Control Center refers to “reliability functional tasks of a RC, BA, TOP or GOP” the drafting team should clarify if these tasks are intended to be the same
Yes
Group
Western Electricity Coordinating Council
Steve Rueckert
WECC believes that the Interchange Coordinator should be removed from the Applicability section of the CIP Version 5 standards. With the new Impact Rating Criteria found in CIP-002-5 Attachment 1, rather than the Risk-Based Assessment Methodology in versions 1-3, an Interchange Coordinator would have no critical assets, and subsequently no critical cyber assets in its role as an Interchange Coordinator. Any assets that meet the criteria in Attachment 1 for an entity registered as an Interchange Coordinator will be owned and operated through its registration as a different functional entity. If the Interchange Coordinator remains in the Applicability section of the CIP Version 5 standards, NERC should clarify the relationship between the currently registered function of Interchange Authority and the function identified in the Functional Model of the Interchange Coordinator.
Individual
John Allen
City Utilities of Springfield, MO
No
Yes
Yes
Yes
Yes
No
No
City Utilities of Springfield, MO agrees with the comments from SPP and APPA.
City Utilities of Springfield, MO agrees with the comments from SPP and APPA.
City Utilities of Springfield, MO agrees with the comments from SPP and APPA.
Yes

Group
ACES Power Marketing
Jason Marshall
No
No
No
Yes
No
Yes
Yes
(1) The clarity of the definition of BES Cyber Asset has been improved greatly. However, we are confused by the statement that a BES Cyber Asset is included in a BES Cyber System. From the background section of CIP-002-5, we thought that the responsible entity had the option of utilizing BES Cyber Systems. If so, then “is included” should be changed to “may be included”. Otherwise, the background section needs to state directly that all medium and high impact BES Cyber Assets must be grouped into BES Cyber Systems. (2) For BES Cyber System, we suggest replacing “to perform” with “to facilitate performance”. Often times, the BES Cyber System is used by a System Operator but the BES Cyber System does not actually perform the reliability task. The System Operator performs the task. An EMS is an excellent example. The EMS does not perform the reliability task. It only facilitates the System Operator performing the reliability task.
(1) We remain unconvinced that a definition of Control Center is needed particularly given that the EOP-008-1 standard regarding backup control centers/functionality was written without a definition. At a minimum, we recommend that the drafting team consult the EOP-008-1 drafting team regarding the definition. (2) If the definition persists, we suggest changing operating personnel to System Operators. System Operators clarifies that it is truly a control center and not a control house at a substation for instance. We also recommend deleting “reliability” or “functional” from the description of tasks. Since the functional model is focused on reliability tasks, they are essentially redundant.
(1) Please change “security procedures developed by the responsible entity” to “security procedures”. Many registered entities utilize consultants to write security procedures. Technically, one could exclude consultant developed security procedures with the current language. (2) While we agree that a safety issue should constitute a CIP Exceptional Circumstance, in general, safety issues are not subject to NERC standards. In this case, an unsafe condition would temporarily exempt the responsible entity from strict compliance with specific requirements identifying a CIP Exceptional Circumstance as an exception. Safety is regulated by other governmental agencies.
For Interactive Remote Access, it is not clear why bullet 1 is needed in the definition. What can be meant by Responsible Entity that is not covered by employees, vendors, contractors or consultants? If the Responsible Entity’s Cyber Asset is used by the employee, vendor, contractor or consultant, it will be covered in bullets 2 and 3. It is also not clear why ownership was added to bullets 2 and 3. Ownership is not relevant. The key is whether the Cyber Asset was used to initiate access.
Reportable BES Cyber Security Incident needs to be coordinated with the Disturbance and Sabotage Reporting standards drafting team.
Yes
(1) Overall, we agree with the implementation plan. However, some changes are needed. The implementation plan needs to clearly state when initial compliance is required for non-periodic requirements. Because there is a list of initial performance requirements for periodic requirements, it is implied that compliance is required for all other requirements on the effective date of the standard.

A direct statement to this effect would be perfectly clear. (2) The purpose of the table listing applicability on the last page to the three types of Cyber Assets is not clear. Their applicability is included in the standard. An explanation before the table would be helpful in understanding its inclusion. (3) The section on Disaster Recovery needs to more clearly state that there is a reasonable expectation that an entity may need a grace period after a significant outage (i.e. widespread outages caused by a hurricane). The section is clear that the focus should be first on recovering the system. However, it seems to imply that a responsible entity should be in compliance immediately following restoration activities. This is not likely as many BES Cyber Systems or BES Cyber Assets may have been replaced or reconfigured (i.e. relays) to accommodate rapid restoration. It will take time to make them compliant after the restoration period.
Individual
Robert Mathews
Pacific Gas and Electric Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Scott Berry
Indiana Municipal Power Agency
No
IMPA believes there needs to be a better feel or definition for what “monitoring and control” means. For instance, does a fax and/or e-mail constitute a manual control or is a manual control performed when a control switch is physically engaged by an operator? Also, if a Control Center is not staffed 24 x 7 x 365 but it does perform the reliability functional tasks of either 1), 2), 3), or 4) during normal work days does this constitute real-time control?? IMPA does not understand how voice instruction is part of the “monitor and operating control function.”(Reference: Frequently Asked Questions Cyber Security Standards CIP-002 – CIP-009 dated May 9, 2005) These terms are too broad and can very easily be defined in multiple ways by multiple people, especially auditors. These terms need to be defined by NERC before inclusion in this proposed standard. For instance, what might help to better define what a Control Center is for a Transmission Operator is to use a “aggregate weighted value” similar to that proposed in Attachment 1, Section 2.5 – there are many smaller entities that may have Transmission Facilities at only two locations that are between 100 kV to 199 kV and have a Control Center staffed during normal work days that will be forced to assign their Control Center a Medium

Impact Rating when is should be Low. When it comes to generation, a Control Center may monitor and control two generation sites that each has 160 MW for peaking use (low capacity factor). Under this condition, the Control Center would be a medium impact when it should be a low impact. Please see IMPA’s recommendation on Form A, question 3 for the definition of Control Center.
Individual
Rolynda Shumpert
South Carolina Electric and Gas
One item that I do not see explicitly addressed in the standards would be how to treat temporary reconfigurations of the system that may elevate an asset that is normally not classified as a BES Cyber System to a higher status. Would a temporary system alignment require that the requirements for a Medium Impact be invoked on that temporary system while it is in that configuration? There are probably other examples of temporary system alignments that could elevate an asset’s impact rating that should be addressed under the CIP standards, or maybe it is already included and I overlooked it when I reviewed the standards.
Group
Western Area Power Administration
Brandy A. Dunn
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Define “Associated Data Centers”
Group
SPP and Member companies
Lesley Bingham
No
Yes
Yes
Yes
Yes
No
Yes
BES Cyber Asset includes a sentence in parentheses which provides an example of what is not a BES Cyber Asset. In the previous version of the standard, this was a stand-alone definition for the term “Transient BES Cyber Asset”. It is more clear to have this defined separately than included in the definition of BES Cyber Asset. Whether it is termed a “Transient BES Cyber Asset” or is given another name is at the discretion of the Standards Drafting Team. A definition should state what a term IS; not what it is NOT.
Protected Cyber Asset includes a sentence in parentheses which provides an example of what is not a Protected Cyber Asset. In the previous version of the standard, this was a stand-alone definition for the term “Transient BES Cyber Asset”. It is more clear to have this defined separately than included in the definition of Protected Cyber Asset. Whether it is termed a “Transient BES Cyber Asset” or is given another name is at the discretion of the Standards Drafting Team. A definition should state what a term IS; not what it is NOT.
Yes
Group
IRC Standards Review Committee
Christine Hasha
Yes
No
Yes
Yes
No
No
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding the BES Cyber Asset definition under question 8.
Regarding the definition of Control Center (question 2), the IRC requests clarification of word

“facility”. Does this include (1) the control room where system operations personnel work; (2) the data center housing the cyber assets; (3) all of a multi-purpose building containing 1 and 2; or (4) all of the above?
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding the CIP Exceptional Circumstance definition under question 10. The IRC respectfully provides these additional comments. The IRC requests modification of the definition of CIP Senior Manager (question 3) to read, “A single senior management official with overall authority and responsibility for the implementation of and continuing adherence to the Responsible Entity’s NERC CIP program”. This is to not imply that it is required that this person “lead” the implementation and ensure involvement beyond initial implementation.
The IRC requests modification of the definition of Physical Access Control Systems (question 4) to replace “exclusive of” with “excluding”.
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding the Interactive Remote Access definition under question 12.
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) under question 13. The IRC respectfully provides these additional comments. The IRC requests modification of the definition of External Routable Connectivity to, “A bi-directional routable protocol connection that is used to access a Cyber Asset within an Electronic Security Perimeter from a Cyber Asset that is outside the Electronic Security Perimeter.”
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) under question 14.
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) under question 16.
Individual
Gregory Campoli
NYISO
No
Yes
Yes
Yes
Yes
No
No
• BES Cyber Asset definition from "it is directly connected to a Cyber Asset within an ESP" to "it is directly connected to a network, or to a Cyber Asset within an ESP"
• Intermediate device location seems too prescriptive as different technology combinations may allow the DMZ and device location to be different that defined.
• Electronic Access Point (“EAP”) A Cyber Asset interface on an Electronic Security Perimeter that allows externally routable bi-directional communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter or inbound communications to a Cyber Asset within the Electronic Security Perimeter.
• Physical Security Event is a suspicious event that is monitored prompting a Physical Security Investigation • Cyber Security Event is a suspicious event that is monitored prompting a Cyber Security Investigation • Physical Security Investigation is the process defined by the entity to investigation events that are identified to the Physical Security controls or impacts the operations of

the facility. • Cyber Security Investigation is the process defined by the entity to investigate events that are identified to the BES Cyber Assets, BES Cyber Assets, Protected Cyber Assets and that are suspicious or may impact the operation of the cyber asset. • Physical Security Incidents are the result of investigations or processes that identify the impact of the event to the Physical Security Perimeter, controls or facility. • Cyber Security Incidents are the results of the investigations or process that identify the impact of the event upon the BES Cyber Asset, BES Cyber System, or Protected Cyber Asset. • Reportable Physical Security Incident is a compromise or interruption to the Physical Security Perimeter, controls or facility. • The definition of Reportable Cyber Security uses the terms "compromised" and "disrupted" plus the phrase "reliability tasks of a functional entity" All three need their own definition/clarification.
No
• Concerned with the Version 3, to Version 4 to Version 5 implementation path and hope FERC and NERC will work to resolve the path forward to minimize implementation risk to the industry • Request clarification on the Disaster Recovery's "completion of the restoration activities" (top of the clean version's page 5). What event/action/etc signifies this completion?
• Section 5 for CIP-003-5 is the only place that explains how to read the bullets and numbers in the Measures. From the second paragraph of Section 5, "Measures provide examples of evidence to show documentation and implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence." Request clarification this bullets and numbers explanations applies to the Requirements and Applicability sections of each of CIP-002-5 - CIP-011-1. If this was the SDT's intent, then recommend this clarification be added to Section 5 of each of CIP-002-5 - CIP-011-1. • General comment – recommend that each Requirement's Part identify that Part's goal
Group
Tri-State G&T - Transmission
Tracy Sliman
Yes
Yes
No
Yes
Yes
Yes
Yes
In definition of CIP Senior Manager replace "CIP Standards" with "CIP-002 through CIP011". In definition of Control Center add 24/7 to the first sentence. "One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …"
Yes
Group
CenterPoint Energy
John Brockhan
No

No
No
No
No
Yes
No
CenterPoint Energy requests clarification on the term “adversely impact” and the point in time when the clock starts for the criteria of “within 15 minutes”. Additionally, the definition for BES Cyber Asset states that “Redundancy shall not be considered when determining availability.” CenterPoint Energy requests clarification on whether this concept has been reasoned for application in a substation environment, specifically in the instance of primary/backup relays and identical redundant systems.
CenterPoint Energy agrees with the comments submitted by EEI regarding a definition for Control Center.
CenterPoint Energy proposes that the definition of CIP Senior Manager is not needed as a glossary term, but is acceptable in the requirement description.
CenterPoint Energy recommends that the term “alert” be removed or replaced with “alarm” in the definition of Physical Access Control Systems.
CenterPoint Energy agrees with the comments submitted by NSRS regarding the definition of “Interactive Remote Access”.
CenterPoint Energy believes “was an attempt” is vague and seeks clarification on how such an attempt will be determined. An alternative would be to delete the phrases “or was an attempt to compromise” and “or was an attempt to disrupt”. CenterPoint Energy also agrees with the comments submitted by NSRS regarding revisions to the definition of “Reportable Cyber Security Incident” and replacement of the term “reliability tasks” with “reliability functions”.
No
CenterPoint Energy recommends a table format for the “Initial Performance of Certain Periodic Requirements”. Also CIP-010-5, Part 3.2 is listed with the “Within 12 calendar months” activities. According to the requirement, it should be performed “once every 36 calendar months”.
Individual
James Tucker
Deseret Power
No
No
No
Yes
Yes
Yes
Yes
Control Center – DESERET POWER is concerned that in this definition the mere presence of a SCADA HMI might be considered a Control Center by a CEA if it could possibly be used to control BES assets in real-time even if an entity does not use it that way. Some of the registered entities do not man these control centers 24/7 and are unable to perform real time control after hours, or any other time that other duties take them 15 minutes away from the computer. In some instances these entities might be registered as TOPs only because they own a limited and discrete 115 kV facility that no other entity was willing to register as a TOP for. Often times this 115 kV facility performs no reliability function. DESERET POWER suggests adding “24/7 to the first sentence of the Control Center definition

as shown in the underlined text: “One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …”
CIP Senior Manager – In this definition replace “CIP Standards” with CIP-002 through CIP-011. If this is not completed, this definition would apply to CIP-001 which still exists and is an unrelated standard. This revision will provide clarity to the limit of the definition.
Yes
Individual
Jennifer Wright
San Diego Gas & Electric
San Diego Gas & Electric (“SDG&E”) proposes the following changes to the definition of “Cyber Security Incident”: “A malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter, or, • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System, or, • Is a violation or imminent threat of a violation of computer security policies, acceptable use policies, or standard security practices impacting or within covered Electronic Security Perimeters or Physical Security Perimeters."
A. Throughout the standards, the terms “data” and “information” are used interchangeably. The term “data” should be used when referring to a collection of facts in any form, and “information” should be used when referring to a message that has been received and understood. B. The CIP standards need to be more closely aligned with the comparable NIST or ISO standards. C. The CIP standards still hold the responsible entity completely accountable with no accountability to the vendors that supply and support the in scope systems. The standards should be made applicable to these third parties, specifically those third parties that are sole providers of products and or services that are needed to comply with NERC CIP standards. The standards also need to apply to organizations; public and private that have access to and or the ability to manage assets that are in-scope for NERC CIP. Past comments have alluded to the fact that utility companies have the ability to choose to engage certain third parties. While this may be the case for certain types of products and or services, this is not factual given stipulations by third parties to manage certain aspects of the grid and or products provided. Examples are turbine maintenance and Cal-ISO connectivity. In addition, Smart Grid will introduce new technologies for the automation of grid activities, whereby third parties and or union affiliates will be responsible for installing, maintaining and or troubleshooting grid technologies that have the potential to be in scope for NERC CIP. D. Comment Form B, Question 2: Although the wording of CIP-004-5, R2 appears to require role based awareness and training, the associated tables appear to apply requirements to systems, not to roles. SDG&E recommends applying awareness and training requirements solely to roles. E. Comment Form B, Question 14: Parts 1.4 and 1.6 of CIP-006-5 Table R1 require controls that monitor Physical Security Perimeters and Physical Access Control Systems twenty four hours a day, seven days a week “with 99.9% availability.” This 99.9% availability is an arbitrary criterion. Does the 99.9% apply per day, per week, per month, or per year?

99.9% equates to an allowable down time of 8.76 hours per year. Physical access control systems can experience momentary loss of connectivity between system servers and local controllers that may result in interruption of alarm monitoring for a few seconds or less. Will each of these momentary interruptions be a violation when they exceed 0.01% in one day/week/month/year? How is this criterion applied to multiple controllers? If 100 controllers have an interruption for one second, is the down time the same as if one controller has an interruption of one second? Part 1.5 of CIP-006-5 Table R1 requires an alarm or alert in response to detected “unauthorized circumvention” of a physical access control into a PSP. “Unauthorized circumvention” seems to imply hostile intent and successful penetration of the PSP access point. Is this the intent?
Group
Seattle City Light
Pawel Krupa
General Comments: SCL does not support the approach proposed in version 5 of the CIP Standards, either as to fundamentals or details. Fundamentally SCL believes the v5 approach is flawed and will introduce significant compliance burden without ensuring cyber security for the BES. Detailed concerns remain as provided previously (please refer to comments submitted by SCL on January 6, 2012). Although today's enforcable CIP Standards share many of the flaws of v5, SCL believes industry would be better served by developing maturity around the existing Standards while developing a new, different approach to cyber security that is based on the established practices and theory of the information technology industry.
Group
PacifiCorp
Sandra Shaffer
PacifiCorp supports the comments submitted by EEI.
Individual
Steve Alexanderson P.E.
Central Lincoln
Yes
No
Yes
Yes

Yes
Yes
Yes
We thank the SDT for removing the circularity and overreach of the prior definition. It occurs to us, however, that the mere presence of a SCADA HMI might be considered a Control Center by a CEA if it could possibly be used to control BES assets in real-time even if an entity does not use it that way. Many of the registered entities do not man these stations 24/7 and cannot perform real time control after hours or any other time that other duties take them 15 minutes away from the computer. In addition, these entities might be registered as TOPs only because they happen to own a piece of 115 kV equipment that no other entity was willing to register as an operator for, even if that device performs no reliability function. We suggest “One or more facilities hosting operating personnel 24/7 that monitor and control the Bulk Electric System (BES) in real-time …”
Yes
Individual
Russell A. Noble
Cowlitz County PUD
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Cowlitz agrees with the comments submitted by APPA. Cowlitz also adds that a Control Center which should be afforded any Medium or High impact assessment should also be manned at all times, i.e., 24/7. There exist small TOP entities whose existence is strictly due to the unwillingness of any neighboring entity to cover for their TO registration. Such TOP entities may only own a few 115 kV devices which have no operational reliability function other than to drop load, or break a transmission loop designed solely to improve local quality of service. Since there is no need to monitor the operational status of such transmission systems in real time, these small entities will only have personnel at the “controls” as needed. Therefore, Cowlitz suggests the definition be changed to include “One or more facilities hosting operating personnel 24/7 who monitor and control the BES in real-time.
Yes

Cowlitz agrees with the comments submitted by APPA.
Cowlitz agrees with the comments submitted by APPA.
Individual
Tony Kroskey
Brazos Electric Power Cooperative
No
No
No
Yes
No
Yes
Yes
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
We thank the SDT for improvements to the draft definitions, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
Yes
We thank the SDT for improvements to the implementation plan. Please see the formal comments of ACES Power Marketing.
Please see the formal comments of ACES Power Marketing.
Individual
Scott Harris
Kansas City Power & Light
No
No
Yes
Yes
No
Yes
Yes

Cyber Assets – The proposed definition uses the description “programmable electronic devices”. The CIP Standard is intended to prevent the compromise of the security awareness and security functions of cyber systems and components through malicious acts either by remote tampering or local tampering. The description of “programmable electronic devices” is too broad a term to use in this definition. There are many devices that could be considered programmable such as program logic controllers, devices that are configurable by firmware changes, and devices that are configurable by hardware switches. None of these devices have operating systems nor interconnectivity through routable protocol that can compromise their intended function. The proposed CIP Standards do not recognize the limits of these devices and subsequently impose unrealistic requirements of change control, account management, electronic user access records, etc. Considering the broad application in the proposed CIP Standards of this definition, this definition needs to be revised to the following: “Electronic devices that can execute code and use a routable protocol to receive or transmit information, including attached peripheral hardware and software installed on those devices.”
Subscribe to the comments submitted on behalf of EEI.
No other comments.
Dial-Up Provide a definition of “dial-up” for clarity in the standards. Proposed Definition: Dial-Up Connectivity – Connectivity to BES Cyber Assets (or associated Protected Cyber Assets) which is publically accessible using the Publically Switched Telephone Network (PSTN). Intermediate Device Modify the definition to allow for Intermediate Devices to terminate on an Electronic Access Point or to be external to the ESP. Rationale – This will ensure applicable Intermediate Devices are not ‘disqualified’ from operating as such should they have an interface which is an electronic access point into the ESP. Associated Electronic Access Control or Monitoring Systems – Applies to each Electronic Access Control or Monitoring System directly monitoring or negotiating access to applicable high impact BES Cyber Systems or medium impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems. Associated Physical Access Control Systems – Applies to each Physical Access Control System directly negotiating access to applicable high impact BES Cyber Systems or medium impact BES Cyber Systems with External Routable Connectivity.
No other comments.
No other comments.
No other comments.
No
Until the scope of the assets and components comes to rest, it is not possible to make a determination that the implementation plan has sufficient time to implement these requirements.
Zero-defect requirements: Many of the CIP standards and requirements involve actions that are repeated hundreds of times such as access reviews, personnel training, access removals, etc. In those instances, the Violation Severity Levels dictate a failure of a single instance is an absolute failure of the requirement and does not recognize the hundreds of successes. In some regards, the current Find, Fix, and Track settlement processes recognize these instances and manage them appropriately. However, the Standards would be greatly improved by incorporating an appropriate ratio of success to failure in the VSL’s thereby recognizing the real risk to the BES.
Individual
Martin Bauer
US Bureau of Reclamation
No
Yes
Yes
Yes
Yes
Yes
Yes

BES Cyber assets for a Blackstart generator or resource smaller than 75MVA shoud not be considered BES Cyber Assets. This may reduce the risk of entities with smaller BES resources removing those resources from restoration plan(s).
Individual
Richard Vine
California Independent System Operator
No
No
No
No
No
No
BES Cyber Asset – Remove the 15 minute criteria as it is believed that it will lower the security of assets by removing them from qualifications. Suggest a table based on functional criteria.
No comments
1. BES Cyber System Information – define what it is meant by “or pose a security threat”. Suggest removing this wording as this is subject to interpretation. 2. CIP Senior Manager – the definition should include the operation and maintenance of the requirements (ongoing compliance). It appears that after the requirements are implemented, according to the implementation plan, that there is no longer a need for a “CIP Senior Manager”. This appears to contradict CIP-003.
Physical Access Control Systems - Replace the word “exclusive” with “excluding”
For Interactive Remote Access reword “…2) Cyber Assets used or owned by employees, and” to “…2) Cyber Assets used by employees”. Employee owned devices should not be allowed to be used for remote access to BES Cyber Assets.
1. Provide examples in the definition for Electronic Access Point and Electronic Security Perimeter. 2. External Routable Connectivity – This should also pertain to Protected Cyber Asset. BES Cyber System is a group therefore the term should be replaced with BES Cyber Asset. The definition should be reword to “A bi-directional routable protocol connection that is ….”. A suggestion for re-writing the definition may look something like “A bi-directional routable protocol connection that is used to access a BES Cyber Asset or Protected Cyber Asset from a Cyber Asset that is outside the associated Electronic Security Perimeter.” 3. Protected Cyber Asset – suggest removing the parenthesis but keep the wording as a separate sentence.
Cyber Security Incident – remove the words “or suspicious event”. Suspicious is too vague and subject to interpretation. Suggest the definition be changed to: “A malicious act that: • Compromises, or was an attempt to compromise a BES Cyber System • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.”
Yes
None
None
Group

Hydro One
Sasa Maljukan
No
Yes
Yes
Yes
Yes
No
No
for clarity, suggest changing the BES Cyber Asset definition from "it is directly connected to a Cyber Asset within an ESP" to "it is directly connected to a network, or to a Cyber Asset within an ESP"
Request clarification on the definition of EAP, must it be routable protocol on both sides?
The definition of Reportable Cyber Security uses the terms "compromised" and "disrupted" plus the phrase "reliability tasks of a functional entity" All three need their own definition/clarification.
No
Although the proposed version 5 implementation plan states that “Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan,” there are concerns that need clarification. The concerns refer to the transition from the currently effective version 3, through version 4 and finally to version 5. Given that (a) the version 4 standards and associated implementation plan were recently approved by FERC; (b) the proposed version 5 implementation plan contains a minimum 24-month period for enforcement means that there will be a period of time during which version 4 would be effective; and (c) when version 4 becomes effective there will be newly identified CAs that will have to be made compliant. In order to comply with version 4 requirements, entities will be need to allocate funding and resources to perform work necessary to become compliant at newly identified facilities. Much of this work must be performed in anticipation of the enforcement date. Once version 5 becomes effective, application of the proposed categorization of BES Cyber Systems may very well result in much of the work done for version 4 compliance being in the end unnecessary.
Request clarification on the Disaster Recovery's "completion of the restoration activities" (top of the clean version's page 5). What event/action/etc signifies this completion?
Section 5 for CIP-003-5 is the only place that explains how to read the bullets and numbers in the Measures. From the second paragraph of Section 5, "Measures provide examples of evidence to show documentationand implementation of the requirement. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence." Request clarification this bullets and numbers explanations applies to the Requirements and Applicability sections of each of CIP-002-5 - CIP-011-1. If this was the SDT's intent, then recommend this clarification be added to Section 5 of each of CIP-002-5 - CIP-011-1. General comment – recommend that each Requirement’s Part identify that Part’s goal