Comment Report

Project Name:	2016-03 Cyber Security Supply Chain Risk Management | CIP-013-1
Comment Period Start Date:	1/19/2017
Comment Period End Date:	3/6/2017
Associated Ballots:	2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 IN 1 ST 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 Non-binding Poll IN 1 NB

There were 134 sets of responses, including comments from approximately 231 different people from approximately 144 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

9. Provide any additional comments for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Luminant - Luminant Energy	Brenda Hampton	6		Luminant	Brenda Hampton	Luminant - Luminant Energy	6	Texas RE
					Stewart Rake	Luminant Mining Company LLC	7	Texas RE
					Alshare Hughes	Luminant - Luminant Generation Company LLC	5	Texas RE
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Chris Gowder	Chris Gowder		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utility Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC

					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steve Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Mark Brown	City of Winter Park	4	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	9	FRCC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Joe McClung	Joe McClung		FRCC	JEA Voters	Ted Hobson	JEA	1	FRCC
					Garry Baker	JEA	3	FRCC
					John Babik	JEA	5	FRCC
MGE Energy - Madison Gas	Joseph DePoorter	4		MRO NSRF	Joseph DePoorter	MGE	1,2,3,4,5,6	MRO

and Electric Co.					Joseph DePoorter	MGE	1,2,3,4,5,6	MRO
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Con Ed - Consolidated Edison Co. of New York	Kelly Silver	1	NPCC	Con Edison	Kelly Silver	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange and Rockland Utilities	NA - Not Applicable	NPCC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion and NextEra	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC

					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Colorado Springs Utilities	Shannon Fair	6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC

					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC
					Shannon Fair	Colorado Springs Utilities	6	WECC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Gray	Board of Public Utilities,KS (BPU)	3	SPP RE
					Shawn Eck	Empire District Electric Company	1,3,5	SPP RE
Santee Cooper	Shawn Abrams	1		Santee Cooper	Tom Abrams	Santee Cooper	1	SERC
					Rene' Free	Santee Cooper	1	SERC
					Bob Rhett	Santee Cooper	5	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC
					Glenn Stephens	Santee Cooper	1	SERC
PPL NERC Registered Affiliates	Shelby Wade	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Charlie Freibert	LG&E and KU Energy, LLC	3	SERC
					Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Dan Wilson	LG&E and KU Energy, LLC	5	SERC
					Linn Oelker	LG&E and KU Energy, LLC	6	SERC
Public Service Enterprise	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF

Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF
Midcontinent ISO, Inc.	Terry BIlke	2		IRC-SRC	Kathleen Goodman	ISONE	2	NPCC
					Ben Li	IESO	2	NPCC
					Terry Bilke	MISO	2	RF
					Greg Campoli	NYISO	2	NPCC
					Mark Holman	PJM	2	RF
					Charles Yeung	SPP	2	SPP RE
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

As stated in FERC Order 829, section 59, “The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations”. R1 does not align with the above FERC directive. FERC clearly insisted that future contracts will address the five attributes of section 59.

If Future is added, the NSRF request that “Future” needs to be better defined. If a company has a contract that is multi-year and each year a new Purchase Order is issued, the contract is not new or revised. There needs to be direction given on how to implement the requirements of the standard going forward.

If Future is not added, then the NSRF request a possible foot note stating… that R1 applies to all contracts (agreements) starting on the date of enforcement of CIP-013-1. As FERC has stated in FERC Order 693, section 253, Entities need to satisfy the Requirements in order to be compliant.

The SDT should update R1 to clearly state this, such as;

“R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to future contracts concerning the procurement of BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: “

This proposed update aligns with FEERC Order 829, section 59 and clearly informs the applicable entity in what is required in future endeavors. R1 will fulfill the FERC directive of having supply chain risk management plans for future procurement, which falls in line with the SDT’s “Notional BES Cyber System Life cycle” model. The NSRF does not agree with the “if applicable” wording and the addition of :” associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets”, as this is not within the FERC Order.

R1.1 and its parts seem to be disjointed. The NSRF understands to have a Plan (R1) to mitigate cyber security risks to the future procurement of BES Cyber Systems, etc. Within the Plan, entities are to use controls in **their** BES Cyber System planning and development “phase” (which is taken as the Entity’s internal processes of wants and needs). To have controls during the “planning and development” phase will not have an impact on the

procurement of a BES Cyber System, etc., since nothing is occurring; this is a planning phase, only. Entities are only discussing their wants and needs. This is similar to the caveat within the NERC Defined term of Operating Instruction; (A discussion of general information and of potential options or alternatives to resolve Bulk Electric System operating concerns is not a command and is not considered an Operating Instruction.) R1.1 has two parts that should address what is required to occur within the plan concerning the objective of R1.1.

Recommend R1.1 to read “The use of controls for BES Cyber Systems to:”

R1.1.1 Identify and assess risk(s) during the procurement and deployment of vendor products and services; and” (unchanged for the proposed draft). This updated wording of R1.1, directs the use of controls within the plan of R1 and R1.1 states use controls to accomplish the attributes of R1.1.1.

Then R1.1.2, states the Entity is to “…**evaluate methods to address** identified risk(s)”. As written, the Entity is to review (address?) their **methods** to mitigate identified risk(s). Without saying, does this part need to be within the proposed Standard? The intent is to mitigate any known risks, not evaluate **methods** to identify risk(s). This could be viewed as an entity’s **method** of industry trends to see what new “processes” there are to “evaluate methods to address identified risk(s). Or is this required in order to keep the “how and what” an entity does up to date and current with known “identify and assess” practices. If so, please clarify.

It may be less ambiguous if R1.1.2 is rewritten to read; “Evaluate mitigation methods to address identified risk(s)”. This clearly supports R1 where the Requirement states “…controls for mitigating cyber security risks…”.

Request that R1.2.parts be updated so Entities will clearly know their expectations under this proposed Standard:

R1.2.1, Process(es) for receiving notification of vendor identified security events; or “Process(es) for receiving notification and release notes of vendor identified security events;

Justification: this updated wording will establish agreed upon processes between the vendor and entity.

R1.2.2, Process(es) for being notified cation when vendor employee remote or onsite access should no longer be granted;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and that the entity need to be kept current on who is authorized by the vendor and allowed by the entity to access BES Cyber Systems.

1.2.3, Process(es) for disclosure of known applicable system vulnerabilities;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and not present a catch 22 when a vendor does not share applicable system vulnerabilities. We also request the “applicable system” be added (as above). Entities may have other vulnerabilities that will not impact the entity’s applicable system.

1.2.4, Coordination of response to vendor-related cyber security incidents;

No change.

1.2.5. Process(es) for verifying software integrity and authenticity of all applicable software and patches that are intended for use;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and relates R1.2.3 since the vendor disclosed a vulnerability. Suggest rewording to ensure that it only applies to situations where the vendor provides means to verify software, since standard does not impose requirements on vendors, Responsible Entity would otherwise be forced into non-compliance.

1.2.6. Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and

No change.

1.2.7. Other pProcess(es) to address risk(s) as determined in Part 1.1.2, if applicable.

Justification: The use of the word “other” is too broad based and could be viewed as all processes, even those outside of the NERC arena. With the clause of “... in Part 1.1.2, if applicable” clearly points to the identified risks of R1.1.2.

Within R1, R1.2, the SDT added the clause, “if applicable” as it relates to EACMS, PACS and PCA’s and the NSRF has concerns with this. As written in the proposed Standard’s rational box, this item is covered in P.59. FERC Order 829, P. 59, in part states:

“59. The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations”.

FERC does not state the use of EACMS, PACS and PCA’s, but rather “…must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations” (emphasis added).

By the SDT interpreting P 59 to mean EACMS, PACS and PCA’s, this unnecessarily expands the scope of this proposed Standard above and beyond the FERC directive. The NSRF views this as, 1) future contracts concerning security concepts and 2) that support BES operations, which is the BES Cyber Systems identified per CIP-002-5.1a, only. Notwithstanding that EACMAS and PACS is not associated with Low impact BES Cyber Systems. Recommend that R1 and R1.2 have the “if applicable, EACMS, PACS and PCA’s” clause deleted. This will allow the Responsible Entity to have their own risk based controls within their supply chain risk management plan(s) based on the definition of BES Cyber System.

Additional NSRF concerns:

The following statement is taken directly from the Rationale for Requirement R1: "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." This, in our opinion, is not conveyed in the written standard's requirement. Though vendors are not intended to be affected by this standard's requirements, Registered Entities will be forced to shy away from purchasing software from companies that cannot meet this standard. We see Regional Entities' Enforcement teams having a difficult time in upholding any possible violations with this standard.

R1. Comments

When it states "if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" what is their intent with the word applicable? It should either be applied or not applied to the systems. If the intent is to give the decision to the Registered Entities make this clearer, or remove the non-BCSs, completely.

R1.1.2 Comments

Add "mitigation" to methods. The intent is to alleviate an identified assessed risk.

Likes 2	Platte River Power Authority, 5, Archie Tyson; OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

- Recommend rewording Requirement 1 to: "Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control

or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets, ***to specifically address the risk of introduction of malicious code through the supply-chain process.*** The plan(s) shall address:" This addition clearly scopes the plan without relying on the title alone to hint at the proper scope.

- Is 1.1.2 only evaluating or is it evaluating and implementing?

Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

The expressions, “Identify and assess risk(s),” in R1.1.1 and, “Evaluate methods to address identified risk(s),” in R1.1.2 are unsuitably vague.

TFE opportunity is needed, nor should there be any obligation to impose measures on vendors (see our “additional comments” responses).

Terms such as, “vendor security event,” should be defined or removed.

R1.2.2 conflicts with CIP-004-6 R5 and should therefore be deleted.

R1.2.5 is largely duplicative of R3 and R5 of the standard. They should be made consistent, or one of them should be deleted.

R1.2.6 is largely duplicative of R4 of the standard. They should be made consistent, or one of them should be deleted.

The R1 Rationale statement that CIP-013-1, “does not require the Responsible Entity to renegotiate or abrogate existing contracts,” implies that no action needs to be taken for existing PEDs. This point should be made explicit in the standard per se, but our “additional comments” concerns would still apply for replacing or upgrading existing equipment.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See APPA's, TAP's, and USI's comments.

Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John

Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	

R1 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R1 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R1 should be rewritten to be only applicable to high and medium impact BES Cyber Systems

Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	No
Document Name	
Comment	

Requirement 1 should state specifically, as to its purpose, to prevent the introduction of malware or malicious code through the supply-chain process.

There should be an official NERC definition of the term ‘Vendor(s)’. Although the Rational and Guidelines for each define the term, there should be a more official definition in order to provide appropriate guidance for the auditors when evaluating compliance to this standard.

What does Requirement 1.1.2 mean? ... The plan(s) shall address: The use of controls … to: Evaluate methods to address identified risk(s). If a risk is identified during procurement and deployment, are we only required to evaluate methods to address those risks – or *address* the risks? This is incredibly confusing and leaves this requirement wide-open to interpretation.

The rational for Requirement R5 is identified as being based on FERC Order 829 (page 48), which specifically addresses Vendor Remote Access to BES Cyber Systems, without respect to applicability – Sections 76-80. Multiple requirements are referenced in Standards CIP-004, CIP-005 and CIP-007 that are only applicable to High and/or Medium Impact BESCS with weaknesses identified by not directly addressing vendor initiated machine-to-machine remote access. In the final sentence of Section 80, it is noted that vendor remote access is not adequately addressed in the ‘Approved’ standards and, therefore, is an objective that must be addressed in the supply chain management plans. Again, there is no reference to applicability, whereas the meat of the directive covers approved standards that reference Medium and High impact BESCS.

The scope and content of the already approved standards is the appropriate place to account for this weakness. A full impact and applicability analysis should be performed prior to proposed modification(s).

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

Change/add language to emphasize that failure to obtain the cyber security controls from a vendor doesn't translate to being out of compliance. Entity should have the ability to mitigate risks posed by vendors. IID feels that the SDT should consider modifications to current CIP standards where the topic is already addressed.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

1. The standard lacks clarity on addressing R1.2 sub-requirements where no relationship of any sort exists between a RE and vendors whose products may be installed on applicable systems.

Many software and hardware components utilized on BES Cyber Systems, associated EACMS, PCA, and PACS systems are provided without any contractual agreement other than acceptance of a End-User-License-Agreement (EULA) upon installation.

For example, the Java Resource Environment, which is provided by Oracle Corporation, is utilized by many products. However, there is no agreement or financial transaction associated with the acquisition of Java.

This is even further complicated where open-source software is utilized for which no formal organization holds responsibility.

Finally, some proprietary software is acquired without any contractual arrangements due to low acquisition costs, such as an SSH client for less than $200.

In the case where there is a lack of relationship and/or financial interest in establishment of a formal agreement, how can RE address the provided requirements?

2. What incentive does a vendor have to disclose their vulnerabilities to a client? Wouldn't this disclosure ultimately serve to publicize the vulnerabilities?

Responsible entities can request this cooperation, but verification that the vendor is disclosing all vulnerabilities is not possible.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 6

Answer	No
Document Name	

Comment

During the CIP-013-1 webinar on Feb 2, the SDT indicated several times that it is not the intention of R1 to force vendors to perform actions so that entities can comply with the standard. R1.2.1, R1.2.2, R1.2.3 would force vendors to develop internal processes to notify entities of any changes relating to the requirements which would force vendors to take independent action to notify entities of any changes. Also, during the procurement phase, why would vendors reveal potential security flaws in their product above and beyond normal security patch notifications while they are competing against other vendors for the entities business? This seems like wishful thinking. Also, entities have processes in place already for other CIP requirements to fully prepare an asset for deployment into the ESP. We don't grab equipment off of the back of the delivery truck and deploy it into the ESP immediately so what is the point of knowing about security flaws in their products during procurement? Any security flaws are probably already addressed with patches that will be downloaded and installed when preparing the asset for deployment. Also, a vulnerability assessment has to be performed against the asset and CIP-007/CIP-005 security controls have to be checked prior to deployment. 1.2.1, 1.2.3, 1.2.4 appear to be redundant with CIP-007 R2 security patch management. Is the SDT expecting vendors to provide information about security/design flaws above and beyond the normal security patch notifications? If so, what kind of information would that be?

1.2.5 is troublesome as well (and it seems to be a duplicate of R3). Entities typically use update or proxy servers to discover and identify applicable security patches. For example, we use Windows Update Server Services to identify patches and roll them out once testing and approvals are complete. Do we need to check the check sums of the identified patches or can we trust that the update servers are authenticating the software?

Likes 0	
Dislikes 0	

Response

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SCE agrees with this requirement in concept. However, as written, this requirement contains several issues that SCE believes should be resolved. The language of CIP-013-1 Requirement R1 does not clearly state what is required and is open to several interpretations. For example, Requirement R1, 1.1 requires the use of controls to identify and assess risks during the procurement and deployment of vendor products and services. However, consistent with the COSO framework, a risk methodology identifies and assesses risks, and controls are used to mitigate those identified risks. In addition, the requirement and its subparts do not define the security objective. This lack of clarity in the language of Requirement R1 may pose issues during audit. We recommend the following language to clarify the requirement consistent with intent of the FERC Order No. 829 directives:

R1. Each Responsible Entity shall define, document, and implement one or more supply chain risk management methodologies(s) that address objectives, risks, and controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The defined methodologies(s) shall define controls used to mitigate the risks of entering into contracts with vendors who pose significant risks to responsible entity's information systems, of procuring products that fail to meet minimum security criteria, and of failing to receive adequate notice from compromised vendors, and shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

1.1 The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:

1.1.1 Process(es) for notification of vendor security events;

1.1.2 Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.1.3 Process(es) for disclosure of known vulnerabilities;

1.1.4 Coordination of response to vendor-related cyber security incidents;

1.1.5 Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

1.1.6 Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and

1.1.7 Other process(es) to address risk(s) as determined, if applicable.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy requests further clarification from the drafting team on R1 and whether it applies to Low impact BES Cyber Assets. Since the current language of the requirement is silent on the level of applicability, an entity may assume that R1 applies to all High, Medium, and Low Impact BES Cyber

Systems. Duke Energy disagrees with the concept of applying R1 to Low Impact BES Cyber Systems. At the outset, Low Impact BES Cyber Systems have been subject to a risk assessment and classified as Low Impact since they pose a minimal threat to the BES. Also, a Responsible Entity is not obligated to have an inventory list of its Low Impact BES Cyber Systems. In the rationale section of R5, it is even mentioned that a list of Low Impact BES Cyber Assets is not required. Without a list of Low Impact BES Cyber Systems, we fail to see how a Responsible Entity could demonstrate compliance with R1. For this reason, coupled with the fact that the Low Impact BES Cyber Systems pose a minimal risk to the BES, we do not believe R1 should be applicable to Low Impact BES Cyber Systems, and the requirement language should reflect the applicability.

Duke Energy requests confirmation that the rationale provided in R1 (and throughout the standard) be included in the standard, even after the standard has been finalized and approved. We feel that some of the language in the rationale is very useful, and that some of the language is warranted in the requirement(s) themselves. Specifically, the phrase used in the rationale of R1:

"Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

We feel that this language is significant enough as it pertains to R1.2 and the possibility of disagreement between an Entity and an external party, that it should be placed somewhere in the standard.

Lastly, we recommend the drafting team consider developing this standard similarly to CIP-002-5.1a with regards to the leveraging of a bright-line model of risk assessment. This will ensure that entities are assessing risk consistently of their vendors and removes the potential disagreement in audit that a regulator finds that the entity's risk determination is incorrect based on a different set of subjective criteria. This was the justification needed to move from the risk-based assessment methodology (RBAM) in CIP Versions 1 – 3 to the bright-line criteria developed in CIP Version 5.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

We have four concerns with the proposed requirement.

First, CIP-013 should follow the other CIP Standards with respect to Low BES Cyber Assets. R1 should clearly exclude Low BES Cyber Assets and refer to R5 for those assets, and all requirements related to Low BES Cyber Systems should be consolidated into R5.

Second, we are concerned that the difference in wording between R 1.1 which refers only to BES Cyber Systems, and R1.2 which includes EACMS, PACS and PCAs, is confusing and can cause inconsistencies in implementation. R1.1, and subsequently R1.2, should be rewritten to help with this. Please consider the following suggestions:

From: *"1.1 The use of controls in BES Cyber System planning and development to:"*

To: *"1.1 The use of controls in planning and development to:"*

From: "*1.2 The use of controls in procuring vendor product(s) or service(s) that address the Following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:"*

To: *"1.2 The use of controls in procuring vendor product(s) or service(s):* "

Third, we believe that the term "cyber security incident" in R1.2.4 should be capitalized to be clear that it is to be interpreted as the NERC-defined term "Cyber Security Incident".

Fourth, for consistency and clarity, we request the term 'supply chain risk management' be 'supply chain cyber security risk management' throughout the standard and guidance.

Likes 2	PPL - Louisville Gas and Electric Co., 6, Oelker Linn; Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

ALAN ADAMSON - New York State Reliability Council - 10

Answer	No
Document Name	

Comment

See NPCC comments.

Likes 0	
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5

Answer	No
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AECI contends that R1 should be separated into two distinct requirements. R1 should be revised to require the Responsible Entity to develop and document supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems... The SDT should then develop an additional requirement (R2) to require the Responsible Entity to implement the documented supply chain risk management plan(s) documented in R1.

In addition to the comments above, AECI supports the following comments submitted by the MRO NRSF:

“As stated in FERC Order 829, section 59, “The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations”. R1 does not align with the above FERC directive. FERC clearly insisted that future contracts will address the five attributes of section 59.

If Future is added, the NSRF request that “Future” needs to be better defined. If a company has a contract that is multi-year and each year a new Purchase Order is issued, the contract is not new or revised. There needs to be direction given on how to implement the requirements of the standard going forward.

If Future is not added, then the NSRF request a possible foot note stating… that R1 applies to all contracts (agreements) starting on the date of enforcement of CIP-013-1. As FERC has stated in FERC Order 693, section 253, Entities need to satisfy the Requirements in order to be compliant.”

Furthermore, AECI urges the SDT to use the supply chain definition from NIST Special Publication 800-53 Rev.4 that was identified in paragraph 32, footnote 61 in this requirement.

Likes 0	
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3

Answer	No
Document Name	

Comment

CHPD has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	No
Document Name	

Comment

Platte River Power Authority (PRPA) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

PRPA does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, PRPA requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify

systems, PRPA believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required, low with a reduced set of requirements to address their lower risk, PRPA requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

PRPA requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

PRPA is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see PRPA’s response to Question #9 for additional information on exceptions).

PRPA notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 PRPA requests changing the word *evaluate* to *determine.*

For R1.2.1 PRPA requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 PRPA requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. PRPA requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

Austin Energy (AE) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

AE does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, XXX requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, XXX believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, XXX requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

AE requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

AE is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see XXX’s response to Question #9 for additional information on exceptions).

AE notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 AE requests changing the word *evaluate* to *determine.*

For R1.2.1 AE requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 AE requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. AE requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 2	Austin Energy, 4, Garvey Tina; Austin Energy, 3, Preston W. Dwayne
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

1. The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined in the standard or added to the NERC Glossary of Terms and capitalized when used.
2. It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.
3. R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:“The entity must document its determination as to

what are the supply chain risks. Once this determination has been made and documented, the audit team's professional judgement cannot override the determination made by the Responsible Entity. "

4. For R1: This requirement requires both the development and the implementation of a plan. We recommend modifying this requirement into three steps which follows the CIP-014 structure – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline. The timeline should use fixed dates or intervals and not dates that are linked to the completion of other compliance activities
5. For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." This should be incorporated into the Requirement itself.
6. For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list "planning, acquisition and deployment" and versions of these terms in the diagram. R1.1 uses "planning and development". The meaning of "development" has not been clarified and is not part of the process addressed by this standard. Suggest that "development" be clarified or removed.
7. The standard as written addresses Vendor Risk Management and no other supply chain risks such as sole source and international dependencies. Suggest changing the name, purpose, and other areas of the standard from supply chain" to "vendor".

8. For R1.1.2:

    i. We recommend changing *evaluate* to *Determine.* We also seek further clarification of the intent. As, written the requirement is ambiguous:

        a. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

        b. to evaluate the effectiveness of mitigating that risk? or;

        c. is it meant to identify what controls you have to mitigate the risks you have?

    ii. The evaluation of methods is a administrative task and similar to other tasks removed from the NERC standards as part of the Paragraph 81 project.

9. For R1.2.1: The words "Security Event" are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then this should be an officially defined term either in the standard or in the NERC glossary. The s definition provided in the glossary is "any identified, threatened, attempted or successful breach of vendor's components, software or systems" and "that have potential adverse impacts to the availability or reliability of BES Cyber Systems" It is unclear if the second portion is meant to be part of the definition. Many cyber systems, like firewalls, are under constant threat and attempts to breach the systems security. Suggest replacing "vendor security event" with "identification of a new security vulnerability". Vendors may not be able to determine if a vulnerability "could have potential adverse impact to the availability or reliability of BES Cyber System". This clause would only be applicable in determining when an entity would notify a vendor.

10. For R1.2.1: Page 6, line 12 of the Guidance and Examples document list both notification of security events from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both types of notifications.

11. For R1.2.1: The requirement for the" process for notification" is very different than the "request vendor cooperation" guidance given on page 6, line 22 of the guidance document.

12. For R1.2.2: The requirement for the "process for notification" is very different than the "request vendor cooperation" guidance given on page 6, line 22 of the guidance document The requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that "A failure of a vendor to follow a defined process is not a violation of this Requirement."

13. Page 6, line 12 of the guidance details the notification of the vendor by the entity. It is unclear that the R1.2.1 requires notification by the entity to the vendor as detail in the guidance document.

14. Recommend that “Security Event” be changed to require the reporting of only newly identified security vulnerabilities.

15. Change 1.2.7 from pointing to 1.1.2 to 1.1.1. Remove 1.2 since 1.2.7 covers 1.2.

16. Do not agree with the current draft language that includes all High, Medium and Low BES Cyber Systems in Requirement R1. Suggests limiting this requirement to High and Medium only as the current Low Impact requirements do not require entities to conduct an inventory of equipment and software or identify systems. As written, this requirement will place additional administrative burden on entities and the impacts are not fully understood. If controls are needed for low impact, suggest moving these to R5 to consolidate all low impact into a single requirement.

17. The SDT needs to make sure that there is no duplication in the standards. Provide guidance on how areas that seem to overlap like Interactive Remote Access and CIP-005.

18. Request the SDT to consider adding the following language from the rationale to the language of the standard “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

19. The Rationale for R1, it states that R1, P1.1 addresses P 56 of Order No. 829. P 56 calls for a risk assessment of the entities internal systems with this language “how a responsible entity will include security considerations as part of its information system planning and system development lifecycle processes”. R1, P1.1.1 calls for a risk assessment of the vendors systems with this language “procurement and deployment of vendor products and services.” The language in the order does not match the language in the standard and therefore suggest that the language be consistent to provide clarity.

20. There could be an impact of contract requirements on the ability of public utilities to piggyback on wide-area contracts such as those of National Association of State Procurement Officials (NASPO) Cooperative, Western States Contracting Alliance (WSCA), Washington State Department of Enterprise Service, and others. Recommend that a exclusion be permitted in the case of such contracts, which are important to provide flexibility and negotiating strength for public utilities throughout the country. Include language that provides an exclusion for contracts that are covered by other laws or regulations.

21. The requirement should not reference the word “mitigation”. Suggest that “mitigate” be replace with “address” as listed in R1.2.

22. Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk?

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

Public Utility District No. 1 of Chelan County (CHPD) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	No
Document Name	

Comment

The Public Utility District No. 1 of Chelan County (CHPD) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk

electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 0	
Dislikes 0	

Response

W. Dwayne Preston - Austin Energy - 3

Answer	No
Document Name	

Comment

I support the comments of Andrew Gallo at Austin Energy.

Likes 0	
Dislikes 0	

Response

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	
Comment	

R1.1 The lack of guidelines and technical basis within a balloted and approved standard itself (not in a separate document) will result in many different interpretations and expectations on how to meet the requirement. As demonstrated in the measures section, the section lacks specificity as potentially every correspondence with a vendor is subject to data request and audit.

Who is the vendor? Is it the manufacturer/software company, the reseller the hardware/software is acquired from, the shipping company, the integrator, others? For temporary staff, is the contract employee a vendor? These are just example questions.

A lack of guidelines and technical basis within the standard itself could result in a broad interpretation of R1.1 that provides higher risk with little or no additional security. As entities will have to guess the auditor's interpretation, it increases the likelihood that a standard will be violated due to poor definition.

R1.2 This requirement should define a specific minimum security standard in a manner that avoids the inefficiencies from hundreds of entities performing the same analysis. This inefficiency adds costs to entities and to vendors for items that will be passed on to entities. As written, only concepts are presented, not a minimum specification that entities and vendors can effectively use to cost effectively demonstrate compliance in a consistent manner across the industry.

Likes 0	
Dislikes 0	
Response	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	
Comment	

We agree with the LPPC/APPA comments.

Likes 0	
Dislikes 0	
Response	

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	
Comment	

CHPD has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP has an active role on the CIP-013 SDT with an employee serving as a member of the team as well as our support staff who are participating in the SDT meetings. In addition, SRP has been engaging in dialogue with peers of trade associations such as LPPC to address the CIP-013 standard development activities.

SRP continues to be a strong supporter of efforts that ensure the security of the Bulk Electric System. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order, while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

SRP does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, SRP requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, SRP believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required for low impact assets, with a reduced set of requirements to address their lower risk, SRP requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

SRP requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

SRP is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see SRP’s response to Question #9 for additional information on exceptions).

SRP notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 SRP requests changing the word *evaluate* to *determine.*

For R1.2.1 SRP requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 SRP requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. SRP requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

No objections to R1.1. Although the actual language of R1.2 seems sound, how does this language in the R1 rationale section , "***For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan***" (Section B, p. 5) manage risks associated with Supply Chain Management vendors? Where is the incentive for an entity to actively pursue vendor negotiations to minimize risks during the procurement phase? Merely adding control elements to an RFP that are not subsequently incorporated through vendor negotiations into a product or Service Level Agreement [SLA] seems to be nothing more than an academic exercise. At a minimum, under the current rationale the entity should provide working documents (as described in M1) of the negotiations process to demonstrate compliance with R1.2?

Likes 0	
Dislikes 0	

Response

John Hagen - Pacific Gas and Electric Company - 3

Answer	No
Document Name	

Comment

The following language from the rational box for Requirement R1 does not seem to incentivize an entity to actively pursue vendor negotiations to minimize risks during the procurement phase.

For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Merely adding control elements to an RFP that are not incorporated through vendor negotiations seems to be nothing more than an academic exercise. At a minimum, under the current rational, the entity should provide working documents of the negotiations process to demonstrate compliance with R1.2. Extending the initial review and update, as necessary

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4

Answer	No
Document Name	

Comment

- The extent of the "supply chain risk management plan" should be more clearly defined. The Requirement language goes beyond what is typically considered "supply chain" activities (i.e. activities involving the transformation of natural resources, raw materials, and components into a finished product that is delivered to the end customer) and includes ongoing operational protections. The Standard should more clearly define what is meant by "supply chain" and limit the associated Requirement to mitigating the associated risks. All other operational related

protections should be addressed within the existing CIP Standard that already cover the related protections (e.g. remote access controls should be included in CIP-007 and not in a supply chain standard).

- The R1 Supply Chain Risk Management plan is applicable to BES Cyber Systems of all impact levels (and any associated EACMS, PACs, and PCAs). The following recommendations are provided:
    - The inclusion of Low Impact BES Cyber Systems in the scope of the Supply Chain Risk Management Plan should be reconsidered. The existing CIP-002-5.1 and CIP-003-6 only requires an entity to identify asset(s) containing Low Impact BCS and does not require a documented inventory of low impact BCS/BCA or even a documented list of system/asset types. The expectations of the Requirement would make it very difficult for an Entity to demonstrate compliance without a list of Low Impact BCS/BCA.
    - If after reconsideration it is still deemed necessary to include Low Impact BCS within the scope of the Supply Chain Risk Management Plan, the supply chain Requirement should be removed from CIP-013 and added to CIP-003 with the rest of the requirements that are applicable to Low Impact BCS. SDTs have made conscious decisions to keep all Requirements applicable to Low Impact BCS within the CIP-003 Standard and not have them sprinkled throughout all the CIP Standards. Additional time should be taken in developing the standard to remain consistent with this approach. (Note: Reference the CIP-003-7i draft CIP Standard related to low impact BES System Transient Cyber Assets.)
- For consistency with other CIP Standards, CIP-003 R1.1 should be expanded to include supply chain risk management as part of the collective cyber security policies to be reviewed and approved by the CIP Sr. Manager at least every 15 months.
- Use of the “Notional BES Cyber System Life Cycle” model is problematic. Entities plan and assess future cyber systems, but acquire, configure, deploy, and maintain individual cyber assets.
- R1 – 1.2.1, 1.2.3, 1.2.4 references to vendor security events, vulnerabilities, and incidents are undefined and potentially overly broad. Auditors may not collectively or individually agree with an individual RE’s assessment of how these terms are defined and used within their R1 Plan.
- R1 – appears to overlap with parts of several existing CIP Standards, including: CIP-003-6 R2 Att. 1, Section 3; CIP-004-6 R4.1 - 4.4 and R5.1 - 5.5; CIP-005-5 R2.1 - 2.3; CIP-007-6 R2.1, R5.1, 5.5, 5.6, 5.7; and CIP-010-2 R1.1. Expanding the scope of these existing CIP programs with a new Standard could unintentionally disrupt or conflict with current security architectures and/or critical operations. FE recommends that the SDT consider making coordinated modifications to the scope and applicability of CIP-003, 004, 005, 007 and 010, at some future date, rather than extending existing requirements to a new Standard, i.e. CIP-013. FE suggests that the scope of the Supply Chain Standard include the administrative controls needed to address Order 829, and the operational and technical security controls remain in the existing CIP standards.
- Measures and Evidence – Since the R1 requires an entity to show that the plan has been implemented, M1 does not adequately describe the evidence required to demonstrate implementation of the plan, i.e. especially for technical sub-requirements. (For example the evidence that an entity has implemented, “1.2.1 Process(es) for notification of vendor security events,” would likely require a process map for how vendor notifications are received, processed and resolved. Additionally, an auditor would likely want a sample of actual dated notifications from several vendors with dated evidence of consistent action and resolution.) FE recommends that the SDT provide additional guidance on evidence types, formats etc… similar to what was provided in CIP-003-6 Attachment 2.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment
Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	

Comment
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	No
Document Name	

Comment
R1, R2, and R5 contain obligations that apply to low impact BES Cyber Systems. With the inherent low risk that comes with these systems, Basin Electric questions whether the same protections for highs and mediums should be applicable to lows, especially in context of R1. Basin Electric would prefer low impact requirements be included in CIP-003 rather than CIP-013. Basin Electric is concerned the inclusion of lows will necessitate maintaining a list of low BES Cyber Systems and possibly a list of low BES Cyber Assets. As stated in FERC Order 829, section 59, “The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations”. R1 does not align with the above FERC directive. FERC clearly insisted that future contracts will address the five attributes of section 59. If Future is added, Basin Electric requests that “Future” needs to be better defined. If a company has a contract that is multi-year and each year a new Purchase Order is issued, the contract is not new or revised. There needs to be direction given on how to implement the requirements of the standard going forward.

If Future is not added, then Basin Electric requests a possible foot note stating… that R1 applies to all contracts (agreements) starting on the date of enforcement of CIP-013-1. As FERC has stated in FERC Order 693, section 253, Entities need to satisfy the Requirements in order to be compliant.

The SDT should update R1 to clearly state this, such as:

"R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to future contracts concerning the procurement of BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: "

This proposed update aligns with FERC Order 829, section 59 and clearly informs the applicable entity in what is required in future endeavors. R1 will fulfill the FERC directive of having supply chain risk management plans for future procurement, which falls in line with the SDT's "Notional BES Cyber System Life cycle" model. Basin Electric does not agree with the "if applicable" wording and the addition of :" associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets", as this is not within the FERC Order.

R1.1 and its parts seem to be disjointed. Basin Electric understands to have a Plan (R1) to mitigate cyber security risks to the future procurement of BES Cyber Systems, etc. Within the Plan, entities are to use controls in **their** BES Cyber System planning and development "phase" (which is taken as the Entity's internal processes of wants and needs). To have controls during the "planning and development" phase will not have an impact on the procurement of a BES Cyber System, etc., since nothing is occurring; this is a planning phase, only. Entities are only discussing their wants and needs. This is similar to the caveat within the NERC Defined term of Operating Instruction; (A discussion of general information and of potential options or alternatives to resolve Bulk Electric System operating concerns is not a command and is not considered an Operating Instruction.) R1.1 has two parts that should address what is required to occur within the plan concerning the objective of R1.1.

Recommend R1.1 to read "The use of controls for BES Cyber Systems to:"

R1.1.1 Identify and assess risk(s) during the procurement and deployment of vendor products and services; and" (unchanged for the proposed draft). This updated wording of R1.1, directs the use of controls within the plan of R1 and R1.1 states use controls to accomplish the attributes of R1.1.1.

Then R1.1.2, states the Entity is to "…**evaluate methods to address** identified risk(s)". As written, the Entity is to review (address?) their **methods** to mitigate identified risk(s). Without saying, does this part need to be within the proposed Standard? The intent is to mitigate any known risks, not evaluate **methods** to identify risk(s). This could be viewed as an entity's **method** of industry trends to see what new "processes" there are to "evaluate methods to address identified risk(s). Or is this required in order to keep the "how and what" an entity does up to date and current with known "identify and assess" practices. If so, please clarify.

It may be less ambiguous if R1.1.2 is rewritten to read; "Evaluate mitigation methods to address identified risk(s)". This clearly supports R1 where the Requirement states "…controls for mitigating cyber security risks…".

Request that R1.2.parts be updated so Entities will clearly know their expectations under this proposed Standard:

Please add clarification to what is meant by vendor “services” as stated in R1.2.

R1.2.1, Process(es) for receiving notification of vendor identified security events; or “Process(es) for receiving notification and release notes of vendor identified security events;

Justification: this updated wording will establish agreed upon processes between the vendor and entity.

R1.2.2, Process(es) for being notified when vendor employee remote or onsite access should no longer be granted;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and that the entity need to be kept current on who is authorized by the vendor and allowed by the entity to access BES Cyber Systems.

1.2.3, Process(es) for disclosure of known applicable system vulnerabilities;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and not present a catch 22 when a vendor does not share applicable system vulnerabilities. We also request the “applicable system” be added (as above). Entities may have other vulnerabilities that will not impact the entity’s applicable system.

1.2.5. Process(es) for verifying software integrity and authenticity of all applicable software and patches that are intended for use;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and relates R1.2.3 since the vendor disclosed a vulnerability. Suggest rewording to ensure that it only applies to situations where the vendor provides means to verify software, since standard does not impose requirements on vendors, Responsible Entity would otherwise be forced into non-compliance.

1.2.7. Process(es) to address risk(s) as determined in Part 1.1.2, if applicable.

Justification: The use of the word “other” is too broad based and could be viewed as all processes, even those outside of the NERC arena. With the clause of “... in Part 1.1.2, if applicable” clearly points to the identified risks of R1.1.2.

Within R1, R1.2, the SDT added the clause, “if applicable” as it relates to EACMS, PACS and PCA’s and Basin Electric has concerns with this. As written in the proposed Standard’s rational box, this item is covered in P.59. FERC Order 829, P. 59, in part states:

“59. The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations”.

FERC does not state the use of EACMS, PACS and PCA's, but rather "…must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations" (emphasis added).

By the SDT interpreting P 59 to mean EACMS, PACS and PCA's, this unnecessarily expands the scope of this proposed Standard above and beyond the FERC directive. Basin Electric views this as, 1) future contracts concerning security concepts and 2) that support BES operations, which is the BES Cyber Systems identified per CIP-002-5.1a, only. Notwithstanding that EACMAS and PACS is not associated with Low impact BES Cyber Systems. Recommend that R1 and R1.2 have the "if applicable, EACMS, PACS and PCA's" clause deleted. This will allow the Responsible Entity to have their own risk based controls within their supply chain risk management plan(s) based on the definition of BES Cyber System.

The following statement is taken directly from the Rationale for Requirement R1: "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." This is not conveyed in the written standard's requirement. Though vendors are not intended to be affected by this standard's requirements, Registered Entities will be forced to shy away from purchasing software from companies that cannot meet this standard. We see Regional Entities' Enforcement teams having a difficult time in upholding any possible violations with this standard.

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	No
Document Name	

Comment

For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

1.

   i. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

   ii. To evaluate the effectiveness of mitigating that risk? or;

   iii. Is it meant to identify the controls in place to mitigate the identified risks?

Revise R1.2.1 as follows, "Process(es) for notification of vendor security events **that affect BES reliability**;"

For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.

It is not clear if R1 applies to High, Medium and Low since R3, R4 and R5 specify the impact level. This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

R1.1 is vague in the language used with terms like “assess risk” and “evaluate”.

Concern that the Entity interpretation can be very different than Auditor interpretation. Once an entity has completed its risk evaluation, this determination cannot be overturned by the Regional Entity.

Requirements overlap with existing CIP standards and create double jeopardy situations. Change 1.2.7 from pointing to 1.1.2 to 1.1.1

The following statements from the R1 Rationale box are important caveats for compliance and should be included in the Requirement text:

- “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”
- “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

Seminole Electric comments submitted by Michael Haff

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx

Comment

See overview comments and comments specific to Req2uirement R1, in attached file.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment

Both the draft guidance document and the “Rationale for Requirement R1” section of the draft Standard contain the statement, “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” However, there is nothing in any Requirement or any Requirement Part containing such language. Language similar to existing technical feasibility language in CIP-002 through CIP-011 should be added.

N&ST considers requirement part 1.2.2 redundant with existing CIP-004-6 Requirements R4 and R5 and recommends that either it be deleted from this Standard or modified to indicate a Responsible Entity may address it with existing CIP-004 access management procedures.

N&ST considers requirement part 1.2.6 redundant with existing CIP-005-5 Requirements R1 and R2 and recommends that either it be deleted from this Standard or modified to indicate a Responsible Entity may address it with existing CIP-005 procedures for Electronic Access Points and for Interactive Remote Access.

N&ST also recommends that all “Vendor remote access” requirements relevant to supply chain management be presented in one top-level requirement, not in two (R1 and R4).

N&ST also recommends that all “Software integrity and authenticity” requirements be presented in one top-level requirement, not two (R1 and R3).

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	

Comment

We recommend the drafting team remove the phrase “if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets” from the language of Requirement R1 and Section 1.2 because, we feel that this language is inconsistent with FERC Order 829 Directive language. Also, we suggest that the drafting team add some clarity to the sub-parts of Section 1.2 so that the industry will clearly know their expectations.

In reference to Requirement R1 and contracts, we suggest that the term “future contracts” be included in the proposed language of the Requirement. Also, we suggest the drafting team develop a definition for the term “future contracts” that would potentially include the phrase “new or modified contracts on or after the date of Enforcement” in the proposed definition.

SPP’s proposed language revision to R1:

“Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to future contracts pertaining to the procurement of the BES Cyber System.”

Finally, we feel that the Measurement and Requirement language is inconsistent with the sub-part language. In the second sentence of the Requirement and Measurement the term “mitigating” is used, and we suggest replacing the term with “addressing”. We need to ensure all of our risk management options are available to us.

Likes 0	
Dislikes 0	

Response

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins

Answer	No
Document Name	

Comment

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. We propose the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and

machine [illegible]

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?
1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.
1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?
1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?
Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and

machine ~~remote access~~ access.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?

1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.

1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?

1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?

Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

We commend the drafting team for attempting to meet the directives and respect their effort and commitment to that end. We agree with now acting FERC chair LaFleur's comments in her dissent on Order 829, "The Commission is issuing a general directive in the Final Rule, in the hope that the standards team will do what the Commission clearly could not do: translate general supply chain concerns into a clear, auditable, and enforceable standard within the framework of section 215 of the Federal Power Act."

We do not agree with the approach in R1 (and R2) of creating "plans" and the intent of the plans to "cover the procurement aspects of all four objectives."

Order 829's four objectives did not include creating "plans." All four of the directives either direct or use examples of specific operational cyber security controls which are best addressed as revisions to CIP-002 through -011.

Standards will not be effective, auditable or enforceable with a CIP-013 standard dueling with CIP-002 through -011 on scope and obligations.

CIP-002 through -011 are the appropriate place to address these operational security controls. These standards establish the least ambiguity in scope of obligations. These standards make granular distinctions based on risk when assigning what BES Cyber Assets are subject to each requirement. The risk distinctions go beyond just low, medium or high impact and incorporate Control Center, External Routable Connectivity and Interactive Remote Access in assigning obligations for requirements.

NERC's Compliance Registry Summary of Unique Entities and Functions as of March 3, 2017, identifies 1,398 unique NERC entities. These entities range from entities with a couple breakers for low impact Facilities (lines), to entities operating gigawatts of low impact generation units to entities operating high-impact Control Centers for thousands of miles of medium impact Transmission Facilities, for example. All have BES Cyber Assets and all have very different risks to the grid and different obligations under CIP-002 through CIP-011.

"Plans" cannot achieve an effective, auditable and enforceable standard for 1,398 NERC entities that address the complicated issues identified in LaFleur's dissent … and certainly not to meet the September 2017 directed deadline.

Industry can at a minimum advance cyber security by revisions to operational security controls in CIP-002 through -011. Other commenters, including EEI, are submitting examples of language as starting points.

We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives' deadlines, NERC and industry should reprioritize SDT teams' work and resources.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. We propose the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and

machine machine remote ac

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?
1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.
1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?
1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?
Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	

- Dominion supports the work that the drafting team has performed to-date and understands that the current draft of CIP-013-1 is continuing to evolve. Dominion has developed extensive comments to allow the drafting team to focus efforts on areas of particular concern with the current draft. Dominion supports the team's continued efforts to bring stakeholder knowledge and expertise together to develop an objective based reliability standard that realistically addresses reliability gaps in the cyber supply chain process.

- Dominion has a concern that the specific risks identified in P57 of FERC Order No. 829 are not included Requirement R1. The term used in the current draft of CIP-013-1, "cyber security risks", is overly broad and should be constrained by the enumerated risks in the FERC order.

Constraining language for the term 'cyber security risks' could include" risks associated with the of procurement and installation of unsecure equipment or software, the risks associated with unintentionally failing to anticipate security issues that may arise due to network architecture or during technology and vendor transitions, and the risks associated with purchasing software that is counterfeit or that has been modified by an unauthorized party."

Dominion recommends the development team consider the following language change for R1:

"Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that include security considerations related to cyber security risks related to procuring and installing unsecure equipment or software, the risk of unintentionally failing to anticipate security issues that may arise due to network architecture, unintentionally arise during technology and vendor transitions, and purchasing software that is counterfeit or that has been modified by an unauthorized party for BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets."

- In addition, Dominion recommends that system applicability should be clearly identified in the Rationale section of the requirement. Specifically, it is recommended that the "to the extent applicable" language should be removed from part 1. 2 and from the Rationale for R1.

- Dominion recommends the following for Parts 1.1.1 and 1.1.2:

    i. Identify and assess cyber security risk(s) to the BES, if any, during the procurement and deployment of vendor products and services; and

    ii. Evaluate methods to address identified risk(s).

- The term "services" in Part 1.2 is very broad and could be interpreted differently by different parties. To ensure consistent understanding of this term, Dominion recommends that the development team place context around the term 'service' as used in requirement R1.2 in a compliance guidance document.

- Dominion recommends that Part 1.2.7 be removed from CIP-013-1. The comprehensive list of risks in Parts 1.2.1 through 1.2.6 appropriately addresses the risk.

- As an alternative to the above recommendations, the development team could consider the following new proposed requirements in lieu of requirement R1 and R2:

R1: Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that include security considerations related to cyber security risks of 1) procuring and installing un-secure equipment or 2) procuring and installing un-secure software, including purchasing counterfeit software, or software that has been modified by an un-authorized party 3) unintentionally failing to anticipate security

issues that may arise due to network architecture, 4) unintentionally failing to anticipate security issues that may arise during technology and vendor transitions for BES Cyber Systems and associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The supply chain plan(s) shall address:

1. 1. Process(es) for notification of vendor security events;

1.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.3. Process(es) for disclosure by the vendor of known vulnerabilities;

1.4. Coordination of response to vendor-related cyber security incidents;

1.5. Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use; and,

1.6. Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s);

R2: The supply chain plan(s) shall include a process whereby any risk identified by the vendor during the purchasing process is assessed, reviewed, mitigating activities evaluated, and actions based on the selected mitigating activities implemented prior to placing the item(s) in service.

R3: The supply chain plan(s) shall be reviewed, updated as necessary, and approved by CIP SM or delegate at least once every fifteen (15) months.

The Rationale should explain that risks 1 and2 are addressed by R1.3 and R1.5, risk 3 by R1.1-R1.4 and R1.6, and risk 4 by R1.2, 1.3, and R1.6. And that the planning and system lifecycle processes are addressed in the order are expected to encapsulate the purchasing process and are covered by R2.

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

In addition to high and medium impact BES Cyber Systems, the applicability of R1 should be clear to include low impact BES Cyber Systems.

SCE&G agrees with the concerns and question raised by the Security Practices Working Group of North American Generator Forum (NAGF) regarding "if applicable":

"The phrase "if applicable" is ambiguous in the language of the main requirement. One reading is that "if applicable" means that the requirement only applies should the device types of associated EACMS, PACS or PCAs actually exist. Another reading is that "if applicable" is based on the risk that an entity places on a particular vendor as part of its documented risk management plan(s). If an entity performs a risk assessment of its vendors and finds

that a vendor is a low or potentially zero risk (coupling a vendor's reputation with their particular usage within an entity), does this mean that an entity could determine that the protections in R1 are therefore "not applicable" and not place any additional expectations on them?"

SCE&G believes the current language of R1 places unacceptable burden on the Regional Entities because the obligations of R1 occur at the end of the supply chain between Regional Entity and its vendor(s). Cyber security risks can occur at any phase of the supply chain(s) and R1 does not clearly demarcate the supply chain(s) where the risk management plan(s) apply. It is not clear how far in the supply chain(s) of a BES Cyber Asset do Responsible Entities need to identify and assess procurement risks. SCE&G is concerned that Regional Entities will be held responsible for assessment and mitigation of risks outside of the Entities' realm of influence over vendor internal processes and vendor's supply chain(s).

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG recommends that the overall structure of the proposed CIP-013 standard be changed to be consistent with CIP-004 through CIP-011 standards (Specifically by applying similar formatting and use of applicability tables to identify the in-scope systems.) NRG recommends that the CIP-013 standard should focus only on R1 and R2. This would allow the operational controls to remain or be placed in the existing CIP standards.

NRG suggests that the drafting team consider the risk impact classification for Requirement R1 as they would with the other Requirements through the Standard. Additionally, we suggest the drafting team remove the phrase "if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" from the language of R1 and section 1.2 because, we think that this language is inconsistent with FERC Order 829 Directive language. Also, we suggest that the drafting team adds some clarity to the sub-parts of Section 1.2 on what are the SDT intentions for the industry in reference to these sub-parts.

In reference to R1 and contracts, NRG suggests that the term "future contracts" be addressed in the requirement language such as: "new or modified contracts" on or after the date of Enforcement. NRG recommends that these terms should be vetted in an implementation plan to include a conversation of initial compliance versus implemented/ongoing compliance (for example, Registered Entities need clear understanding of the scope as it pertains to plan reviews, new contracts, modified contracts, current contracts).

The Measurement and Requirement language is inconsistent with the sub-part language. In the second sentence of R1's Measures section, the term "mitigating" is used and we suggest replacing the term with "addressing". NRG recommends that the term "addressing" includes that Registered Entities have the flexibility to exercise all risk management options within a Risk Management Plan (to include an acceptance of risk).

Each requirement should have a provision that allows an entity to accept the risk of selection a vendor that will not or cannot supply a control. The requirement intent appears to be about control of a process of disclosure and communication (how a vendor notifies us). Whether a vendor fixes a vulnerability does not appear to be the direct scope or intent of the requirement. Therefore, obtaining specific controls in the negotiated contract may not be feasible. In these cases, NRG suggests that a failure to obtain and implement these controls is not considered a failure to implement an entity's plan. NRG recommends that an entity be able to use a formalized risk management process to evaluate or accept the risk [Risk Management Plan]. In the event that a vendor cannot supply a control, that a Registered Entity may be able to present a mitigating control or that the Registered Entity be allowed to decide to accept the risk (for example a process to vet through a Registered Entity risk management, supply chain, and/or senior management departments and a process to accept risk based on a risk matrix). This may be implied by R1.2.7; however NRG recommends that the standard explicitly communicate that a level of risk acceptance can be part of an entities' Risk Management Plan. The Risk Management Plan could

include steps to keep track of failures and steps to take in the event that vendor controls are found to be insufficient (for example, lessons learned feedback and correction process) - in the Measures section. An example of demonstration of compliance could be a periodic (i.e. 15 month) survey to the vendor during plan review (i.e. 15 month) validation of the notification processes between the two parties or dependent on the level or risk. NRG recommends that R1 should have a description of elements of a good Risk Management Plan (Measures) to include how deficiencies will be addressed, regular feedback to the vendor, and potential implications of non-conformance. NRG requests clarity on how revisions to the Risk Management Plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

For R.1.2.7, NRG recommends using “or” vs “and” after R1.2.6

In R1.2, NRG recommends rewording the requirement to “implement processes that describe controls to address risks identified in R1.1.” NRG recommends that the intent of R1 to be to provide processes (for disclosure and responding controls). Therefore, NRG recommends that the Measure be limited to the sufficiency of the Entities’ vendor controls and evaluation process. The Measures should state that the evaluation would be on an entities process for evaluation and if a vendor does not uphold a negotiated communication process, this does not reflect a compliance violation on the Registered Entity.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

1. The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined.

2. It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.

3. R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:

“The entity must document its determination as to what are the supply chain risks. Once this determination has been made and documented, the audit team’s professional judgement cannot override the determination made by the Responsible Entity. “

4. For R1: This requirement requires both the development and the implementation of a plan. Recommend breaking this into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement plan in future contracts.

5. For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” This should be incorporated into the Requirement itself.

6. For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list “planning, acquisition and deployment” and versions of these terms in the diagram. R1.1 uses “planning and development”. The meaning of “development” has not been clarified and is not part of the process addressed by this standard. Suggest that “development” be clarified or removed.

7. For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

    i. Is the intent to have the entity evaluate potential methods to mitigate risk? or;
    ii. To evaluate the effectiveness of mitigating that risk? or;
    iii. Is it meant to identify the controls in place to mitigate the identified risks?

8. For R1.2.1: The words “Security Event” are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then” Security Event” should be replaced or clarified in the Requirement. This clarification could include “any identified, threatened, attempted or successful breach of the vendor’s components, software or systems used in the support of the Entity’s BES Cyber System.” This new language differentiates R1.2.1 from the vulnerabilities in R1.2.3
9. For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.
10. For R1.2.2: The requirement for the” process for notification” is very different than the “request vendor cooperation” guidance given on page 6, line 22 of the guidance document the requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that “A failure of a vendor to follow a defined process is not a violation of this Requirement.”
11. Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk
12. Requirements overlap with existing CIP standards and create double jeopardy situations. Change 1.2.7 from pointing to 1.1.2 to 1.1.1
13. The following statements from the R1 Rationale box are important caveats for compliance and should be included in the Requirement text:

“Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

“Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	

Comment

Same as RoLynda Shumpert's comments from SCE&G:

In addition to high and medium impact BES Cyber Systems, the applicability of R1 should be clear to include low impact BES Cyber Systems.

SCE&G agrees with the concerns and question raised by the Security Practices Working Group of North American Generator Forum (NAGF) regarding “if applicable”:

“The phrase “if applicable” is ambiguous in the language of the main requirement. One reading is that “if applicable” means that the requirement only applies should the device types of associated EACMS, PACS or PCAs actually exist. Another reading is that “if applicable” is based on the risk that an entity places on a particular vendor as part of its documented risk management plan(s). If an entity performs a risk assessment of its vendors and finds

that a vendor is a low or potentially zero risk (coupling a vendor's reputation with their particular usage within an entity), does this mean that an entity could determine that the protections in R1 are therefore "not applicable" and not place any additional expectations on them?"

SCE&G believes the current language of R1 places unacceptable burden on the Regional Entities because the obligations of R1 occur at the end of the supply chain between Regional Entity and its vendor(s). Cyber security risks can occur at any phase of the supply chain(s) and R1 does not clearly demarcate the supply chain(s) where the risk management plan(s) apply. It is not clear how far in the supply chain(s) of a BES Cyber Asset do Responsible Entities need to identify and assess procurement risks. SCE&G is concerned that Regional Entities will be held responsible for assessment and mitigation of risks outside of the Entities' realm of influence over vendor internal processes and vendor's supply chain(s).

Likes 0	
Dislikes 0	

Response

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. We propose the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and

machine machine remote ac

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?
1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.
1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?
1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?
Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	

Comment

1) The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined.

2) It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.

3) R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:

“The entity must document its determination as to what are the supply chain risks. Once this determination has been made and documented, the audit team’s professional judgement cannot override the determination made by the Responsible Entity. “

4) For R1: This requirement requires both the development and the implementation of a plan. Recommend breaking this into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement plan in future contracts.

5) For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” This should be incorporated into the Requirement itself.

6) For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list “planning, acquisition and deployment” and versions of these terms in the diagram. R1.1 uses “planning and development”. The meaning of “development” has not been clarified and is not part of the process addressed by this standard. Suggest that “development” be clarified or removed.

7) For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

{C}a. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

{C}b. To evaluate the effectiveness of mitigating that risk? or;

{C}c. Is it meant to identify the controls in place to mitigate the identified risks?

8) For R1.2.1: The words “Security Event” are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then ”Security Event” should be replaced or clarified in the Requirement. This clarification could include “any identified, threatened, attempted or successful breach of the vendor’s components, software or systems used in the support of the Entity’s BES Cyber System.” This new language differentiates R1.2.1 from the vulnerabilities in R1.2.3

9) For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.

10) For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given on page 6, line 22 of the guidance document The requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that “A failure of a vendor to follow a defined process is not a violation of this Requirement.”

11) Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk?

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy believes requirement R1 should only be applicable to BES Cyber Systems and recommends removing the portion of the requirement in R1 and R1.2 that states “and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets”. The FERC order is focused on “industrial control system hardware, software, and services associated with bulk electric system operations” and does not mention Electronic Access Control and Monitoring System (EACMS), Physical Access Control System (PACS), or Protected Cyber Assets (PCA). These additional systems are low risk and not considered industrial control systems. CenterPoint Energy recommends taking a risk-based approach as stated in the FERC order, so entities can focus their efforts on the supply chain risk management of BES Cyber Systems, which pose a higher risk to the Bulk Electric System. Additionally, this requirement is applicable to High, Medium, and Low Impact BES Cyber Systems, but Low Impact BES Cyber Systems do not have EACMS, PACS, and PCA.

If the intent of R1 is address the procurement controls, CenterPoint Energy recommends stating that in the main R1 requirement; otherwise, the sub-requirements in R1 can appear to be duplicative of the technical operational controls in R3 and R4. Furthermore, the expectation for R1 is not clear for open source products with no vendor or products bought off the shelf with no purchase contract.

CenterPoint Energy recommends deleting R1.1.2 as the items in R1.2 appear to be the mitigation for the risks identified in R1.1. There is no need for a separate statement about mitigation in R1.1.2.

R1.2.1 uses the term “security events” which is not defined and the meaning could vary for each vendor. CenterPoint Energy recommends defining the term for consistency.

R1.2.2 appears to be redundant to CIP-004 R5.1 and R5.2 and extends to PACS and PCA requirements formerly required only for BES Cyber Systems (BCS) and Electronic Access Control and Monitoring Systems (EACMS).

R1.2.4 should capitalize the term “cyber security incident” because it is a NERC defined term.

R1.2.5 includes “all software and patches” which conflicts with the existing CIP Standards.

R1.2.6 is either redundant with or in conflict with CIP-005 requirements to identify inbound and outbound access permissions with reason for access and control remote access with 2 factor authentication and an identified access control system. It is unclear what additional evidence would be expected to satisfy this requirement.

R1.2.7 is far too broad, requiring and exposing to audit a potentially infinite number of new processes. The requirement wording is not appropriate for a Reliability Standard.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Ballard Mutters - Orlando Utilities Commission - 3

Answer	No
Document Name	

Comment

OUC has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

OUC does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, OUC requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, OUC believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, OUC requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

OUC requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

OUC is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see OUC's response to Question #9 for additional information on exceptions).

OUC notes that the Rationale for R1 includes a definition of the term "vendors". This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 OUC requests changing the word *evaluate* to *determine.*

For R1.2.1 OUC requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 OUC requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. OUC requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

At the main Requirement level, while the rationale for Requirement R1 clearly states,

"Implementation of the cyber security risk management plan(s) ***does not require*** *the Responsible Entity to renegotiate or abrogate* ***existing contracts****, consistent with Order No. 829 (P. 36) as specified in the Implementation Plan",*

the requirement language is silent to this stipulation and therefore could lead to future confusion if left absent from the requirement language.

For ultimate clarity, ATC recommends the SDT consider the inclusion of language within the Requirement R1 itself that provides this specificity of scope. Proposed language for consideration could include phrasing like, but not limited to:

"Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) for ***new/future vendor/supply chain contracts, agreements, and/or relationships*** *that address controls for mitigating…"*

Additionally, it is not uncommon for operational technology to be proprietary, and as such to limit the supplier base and/or the industry's options/bargaining power over supplier practices. While the Rationale provided by the SDT carries the message that the intent is for this requirement to be forward-thinking and exclude existing contracts, even if the above proposed language were incorporated for clarity, it does not address the gap incurred after initial enforcement and implementation is achieved. Once the Standard would be enforceable, inevitably existing contracts will continue to age and will need to be renewed or renegotiated. This requirement language does not address that condition, the feasibility of the imposed obligations upon the future expiration of existing contracts, nor the potential unintended consequences that may be incurred at the time that renewal or renegotiation process are initiated as those existing contracts reach maturity and ultimately expiration. Consequently, the industry must assure that any future regulations regarding supply chain are constructed in a manner that 1.) supports successful and ongoing accomplishment of safe, secure,

resilient, and reliable operation of the Bulk Electric System as existing contracts reach maturity and inevitably age to the level of expiration, 2.) prevents the unintended consequences that are at variance with the intent to maintain safe, secure, resilient, and reliable operation of the Bulk Electric System.

As an example, some unintended consequences could include, and may not be limited to:

- Rendering previously contracted and necessary suppliers inviable upon the renewal or renegotiation of expiring/expired contracts creating a gap in the ability to procure necessary limited or proprietary supply that supports reliable operations,
- The industry being subject to the operationally risky, unnecessarily time-constrained, and cost prohibitive need to perform wholesale replacements of infrastructure with a new supplier to achieve compliance,
- The industry being held hostage by its suppliers through cost prohibitive supplier capitalization via unreasonable increase to the cost of supplier services containing contractual language that meet the CIP-013-1 requirements for their products/services.

The absence of a provision to accommodate for these potential conditions could lead to an impossibility of compliance and/or could compromise reliability if the Registered Entity 1.) cannot procure necessary products without being subject to a compliance violation, or 2.) is forced to abandon current solutions and perform wholesale upgrades or replacements of BES Cyber System infrastructure in order to comply, 3.) is forced to pay exorbitant fees to renegotiate/renew contracts with limited suppliers of necessary limited or proprietary products. Proposed language for consideration could include phrasing like, but not limited to:

"Each supply chain risk management plan(s) shall contain provisions to address instances where expired/expiring vendor/supply chain contracts, agreements, and/or relationships cannot be reasonably renewed in a compliant mode without posing significant risk to safe, secure, resilient, and reliable operation of the Bulk Electric System and its BES Cyber Assets."

Requirement R1:

The scope of R1 is too broad in its reference to BES Cyber Systems without consideration of impact-rating. Consequently, some of the proposed requirements are duplicative of existing requirements for high and/or medium impact BES Cyber Systems, and others exceed the controls required for approved and future enforceable CIP Cyber Security Reliability Standards for low impact BES Cyber Systems.

1. This approach is at odds with the overall intent for the CIP Cyber Security Standards to be constructed in a manner that applies graduated controls commensurate with the risk associated to the impact rating of the BES Cyber System.
2. This approach creates double jeopardy in certain instances, and is at variance with the approach to the body of documentation that comprises the CIP Cyber Security Standards wherein significant effort was invested to eliminate cross references and duplicative content.
3. Through it redundancy, this approach is at odds with the efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate requirements are administrative in nature only and therefore that do not provide security or reliability value.
4. This approach is at odds with the directive in FERC Order No. 829 (P.2), which directed NERC to draft a new or modified Reliability Standard wherein "…In making this directive, the Commission does not require NERC to impose any specific controls, nor does the Commission require NERC to propose "one-size-fits-all" requirements.

Requirement R1 Sub Requirement 1.1.2:

At the sub requirement level, R1 sub requirement 1.1.2 is broad and unclear. ATC recommends the SDT consider providing clarification if anything actionable is expected beyond just an evaluation, such as creating a plan to address the risk and then mitigating risk where possible.

Requirement R1 Sub Requirement 1.2.2:

R1.2.2 is simultaneously duplicative and additive to the language and/or intent of existing approved and effective CIP Cyber Security Reliability Standards as consequence of the broad reference to BES Cyber Systems without consideration of impact-rating in Requirement R1.

1. CIP-004-6 R4 and R5 address access management and revocation for **individuals** having cyber or unescorted access to specified high and/or medium impact-rated BES Cyber Systems and associated Cyber Assets. The existing enforceable CIP-004-6 standard is silent to the capacity with which a given individual is engaged with a Registered Entity, and therefore in its silence addresses employees, contractors, interns, apprentices, and even vendors or suppliers etc. The existing implemented access requirements within CIP-004-6 are more prescriptive than what is proposed for CIP-013-1 rendering CIP-013-1 R1.2.2 superfluous. Consequently, CIP-013-1 R1.2.2 adds no value and rather creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-004-6 R5. Through it redundancy, this approach is also at odds with the efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate requirements are administrative in nature only and therefore that do not provide security or reliability value.

2. CIP-003-6 R1.2 prescribes policy level controls, and CIP-003-6 R2 Attachment 1 Sections 2-3 necessitate plans for the implementation of physical and electronic controls for low impact BES Cyber Systems. CIP-013-1 R1.2.2 effectively expands the scope and requirements for access of vendor employees beyond what is mandated as access requirements of low impact BES Cyber Systems to all other types of employees and Registered Entity engagements wit personnel. Any expansion in scope to access requirements or controls for low impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

3. Additionally, the inclusion of “onsite access” within the proposed language in 1.2.2 is an expansion in scope from the **second directive** in FERC Order No. 829 (P.2), which directed NERC to draft a new or modified Reliability Standard that “…should address the following security objectives, discussed in detail below: (1) software integrity and authenticity; **(2) vendor remote access**; (3) information system planning; and (4) vendor risk management and procurement controls.”

Requirement R1 Sub Requirement 1.2.4 and 1.2.6:

For consistency with other 1.2.x sub requirements, ATC recommends the SDT consider replacing ‘Coordination’ with ‘Process’ by revising the language in both R1.2.4 and R1.2.6 to “**Process** to respond to vendor-related….”, and “**Process** to implement remote access controls…”, respectively.

Requirement R1 Sub Requirement 1.2.5:

CIP-013-1 R1.2.5 is heavily dependent on supplier capabilities and their willingness to provide tools and/or mechanism to enable Registered Entities to perform integrity or authenticity verification. ATC recommends the SDT consider incorporating language that provides flexibility where it is not technically possible.

Likes 0	
Dislikes 0	

Response

Brian Bartos - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	No
Document Name	
Comment	

1. We are concerned about the risks associated with BES Cyber Asset products and services that may contain potentially malicious functionality, are counterfeit, or are otherwise vulnerable due to poor manufacturing and development practices within the industrial control system supply chain. However, the proposed draft standard extends well beyond software authenticity and beyond the ability for entities to manage.

2. New requirements for notification of changes in supplier workforce and incident reporting are impossible to implement and audit due to a lack of a consistent approach and application amongst entities. Industry and industrial supply chain vendors would serve more time sending out notification agreements and attestations than working on making a better and more secure product. Would the supply chain vendor be required to send out a notification every time an employee leaves or finds a virus in the office? If so, then the requirement will be too burdensome for vendors and entities to manage.

3. We believe NERC language in the in the draft standard would have a significant negative impact on the industrial control system community over the long term. As seen in the nuclear industry, specific standards that are outside of other critical sectors will only drive cost up and a willing supply of vendors, down.

4. The need for such a broad set of requirements are unnecessary due to the existing requirement for the entity to have an incident response plan, anti-virus protection and patch management.

5. The additions of *"and, if applicable,* 4 *associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and* 5 *Protected Cyber Assets" in requirement 1 greatly expands the scope of cyber assets.* ACES recommends limiting the cyber assets in scope to BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the Cyber Security Supply Chain Management Technical Conference on November 10, 2016.

As part of Supply Chain Risk Management, Reclamation understands that the risks associated with interaction with vendors, their products, and/or their services are to be considered and mitigated with controls such as contract clauses, physical controls, and/or electronic controls (including vendor remote access). Reclamation recommends that Requirement R1 should instead address the development of one or more supply chain risk management plans that identify risks and controls for mitigating cyber security risks throughout the life cycle(s) of BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

Within Requirement R1, the life cycle steps to consider in identifying risks and the respective controls should include but not be limited to: evaluation of design, procurement, acquisition, testing, deployment, operation, and maintenance.

Within each Requirement, the sub-requirements should distinguish between high, medium, and low impact BES Cyber Systems and other supporting systems. Reclamation recommends the implementation plan enforcement dates be staggered based on high, medium, and low impact for auditing purposes and to allow the associated risks and severity levels to be spelled out more clearly.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

Rationale for Requirement R1:

The rationale language for R1 states, “The cyber security risk management plan(s) specified in Requirement R1 apply to BES Cyber Systems." If the intent of the “BES Cyber Systems” reference is to be applicable for all three impact classifications (High, Medium and Low), IPC recommends adding impact classification language.

The rationale language for R1 states, “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.” How does the SDT expect Responsible Entities to demonstrate compliance if existing contracts are acceptable?

The rationale language for R1 states, “The objective of verifying software integrity and authenticity (Part 1.2.5) is to ensure that the software being installed in the applicable cyber system was not modified without the awareness of the software supplier and is not counterfeit.” How does the SDT expect Responsible Entities/vendors to demonstrate compliance with this?

The rationale language for R1 states, “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P. 36) as specified in the Implementation Plan." IPC suggests including the verbiage “with vendors, suppliers or other entities executed as of the effective date of CIP-013-1” to the third paragraph of the “Rationale for Requirement R1.”

R1

The requirement language for R1 states, “Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated EACMS, PACS and PCAs.” If the intent of the “BES Cyber Systems” reference is to be applicable for all three impact classifications (High, Medium and Low), IPC recommends adding impact classification language. In addition, if the intent of the “if applicable” reference is to imply “EACMS, PACS and PCAs associated with BES Cyber Systems,” IPC recommends replacing the “if applicable” language with “and their associated” language to remain consistent with current enforceable standard language.

R1.2 – IPC has concerns about the ability of a Responsible Entity to comply with, as written, R1.2, specifically R1.2.1 – R1.2.7. IPC believes there will be instances when vendors (e.g., larger IT vendors, smaller vendors, open source software, etc.) will not agree to provide all of the information necessary to meet the R1.2.1 – R1.2.7 requirements, potentially forcing Responsible Entities to look at other, lower quality options to ensure compliance, or vendors will use the required compliance control(s) as leverage during contract negotiations. The rationale for R1 states, “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan.” However, the rational language does not translate to a release from the R1.2 requirements. How does the SDT foresee Responsible Entities demonstrating compliance when an entity is unable to obtain a specified control(s)? Further, how does the SDT foresee these requirements being measured by auditors?

R1 and R1.2 require the development and implementation of “processes” and/or “plans.” If vendors refuse to agree to terms, what implementation evidence does the SDT expect Responsible Entities to provide? Additionally, if the vendor agrees to the terms stated but fails to deliver according to the documented process, does the SDT foresee this being viewed as non-compliance?

IPC would like to know what additional security measures R1.2.1, R1.2.3, and R1.2.4 provide that aren’t already covered by CIP-007-6, for example CIP-007-6 R2?

IPC recommends adding mitigation plan verbiage to R1.2 requirement language.

M1

The measure language for R1 states, “Evidence shall include (ii) documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, written agreements in electronic or hard copy format, correspondence, policy documents, or working documents that demonstrate implementation of the cyber security risk management plan(s).” How will this measure apply to Responsible Entities who do not renegotiate or abrogate existing contracts or are unable to obtain specific controls?

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

Santee Cooper does not agree with including all BES Cyber Systems in Requirement R1 and suggest using a risk-based approach, to limit this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, Santee Cooper believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, Santee Cooper requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

Santee Cooper requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

Santee Cooper is concerned about compliance obligations for procurement activities associated with system integrators. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they provide important negotiating strength, flexibility, and effectiveness in contracting (see Santee Cooper’s response to Question #9 for additional information on exceptions).

Santee Cooper notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used. Additionally, Santee Cooper requests that the term be used consistently throughout the standard and not switch between vendor and supplier.

For R1.1.2 requests changing the word *evaluate* to *determine.*

For R1.2.1 Santee Cooper requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. Santee Cooper requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

In Measure M1, Santee Cooper requests that the language be changed to be consistent with the Requirement. Specifically, change “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…” to “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…” (BOLD emphasis added). The construction “address risk” conforms to the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as opposed to mitigated.

Santee Cooper requests that the title of the standard be changed to “Vendor Risk Management” to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term “supply chain risk management” encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although

the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, LCRA requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, LCRA believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, LCRA requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes CIP-013-1 R1 should only apply to High and Medium cyber systems. Applicability to Low systems would potentially place a large burden as current Low Impact requirements do not require entities to conduct an inventory of equipment and software or identify systems. BPA requests that the SDT provide clarification as to how R1 would apply to TCAs. 1.2.1 - Is notification under 1.2.1 for what is known at the time of procurement or does it persist after the procurement is fulfilled? What is the time limit? BPA proposes that the language be made consistent with the R1 rationale: “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”	

1.2.2 through 1.2.6 – BPA believes this expands the scope of CIP-004 R5. BPA requests clarification on what this applies to: does it apply to the vendor or to the hardware/software?

The SDT should address gaps that apply to other standards within that standard and not group them into CIP-013-1. For the sub-parts of CIP-013 R1, the scope might be more appropriate in the following locations:

- The topic of access control CIP-013 R1, P1.2.2 is addressed in CIP-004 R5, P5.1
- Vulnerability assessments CIP-013 R1, P1.2.3 is addressed in CIP-010 R3, P3.1
- Cyber security response CIP-013 R1, P1.2.4 is addressed in CIP-008 R1, P1.1
- Software security patches CIP-013 R1, P1.2.5 is addressed in CIP-007 R2, P2.1-2.4; BPA suggests revision to address all patches.
- Interactive Remote Access CIP-013 R1, P1.2.6 is addressed in CIP-005 R2, P2.1.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

1) The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined in the standard or added to the NERC Glossary of Terms and capitalized when used.

2) For R1: This requirement requires both the development and the implementation of a plan. We recommend modifying this requirement into three steps which follows the CIP-014 structure – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline. The timeline should use fixed dates or intervals and not dates that are linked to the completion of other compliance activities

3) The standard as written addresses Vendor Risk Management and no other supply chain risks such as sole source and international dependencies. Suggest changing the name, purpose, and other areas of the standard from supply chain” to “vendor”.

4) For R1.1.2:

a. We recommend changing *evaluate* to *Determine.* We also seek further clarification of the intent. As, written the requirement is ambiguous:

i. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

ii. to evaluate the effectiveness of mitigating that risk? or;

iii. is it meant to identify what controls you have to mitigate the risks you have?

b. The evaluation of methods is a administrative task and similar to other tasks removed from the NERC standards as part of the Paragraph 81 project.

5) For R1.2.1: The words “Security Event” are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then this should be an officially defined term either in the standard or in the NERC glossary. The s definition provided in the glossary is “any identified, threatened, attempted or successful breach of vendor’s components, software or systems” and “that have potential adverse impacts to the availability or reliability of BES Cyber Systems” It is unclear if the second portion is meant to be part of the definition. Many cyber systems, like firewalls, are under constant threat and attempts to breach the systems security. Suggest replacing “vendor security event” with “identification of a new security vulnerability”. Vendors may not be able to determine if a vulnerability “could have potential adverse impact to the availability or reliability of BES Cyber System”. This clause would only be applicable in determining when an entity would notify a vendor.

6) For R1.2.1: Page 6, line 12 of the Guidance and Examples document list both notification of security events from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both types of notifications.

7) For R1.2.1: The requirement for the” process for notification” is very different than the “request vendor cooperation” guidance given on page 6, line 22 of the guidance document.

8) Page 6, line 12 of the guidance details the notification of the vendor by the entity. It is unclear that the R1.2.1 requires notification by the entity to the vendor as detail in the guidance document.

9) Recommend that “Security Event” be changed to require the reporting of only newly identified security vulnerabilities.

10) Change 1.2.7 from pointing to 1.1.2 to 1.1.1. Remove 1.2 since 1.2.7 covers 1.2.

11) Do not agree with the current draft language that includes all High, Medium and Low BES Cyber Systems in Requirement R1. Suggests limiting this requirement to High and Medium only as the current Low Impact requirements do not require entities to conduct an inventory of equipment and software or identify systems. As written, this requirement will place additional administrative burden on entities and the impacts are not fully understood. If controls are needed for low impact, suggest moving these to R5 to consolidate all low impact into a single requirement.

12) The Standard drafting team needs to verify that the SDT needs to make sure that there is no duplication in the standards. Provide guidance on how areas that seem to overlap like Interactive Remote Access and CIP-005.

13) Request the SDT to consider adding the following language from the rationale to the language of the standard “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

14) The Rationale for R1, it states that R1, P1.1 addresses P 56 of Order No. 829. P 56 calls for a risk assessment of the entities internal systems with this language “how a responsible entity will include security considerations as part of its information system planning and system development lifecycle processes”. R1, P1.1.1 calls for a risk assessment of the vendors systems with this language “procurement and deployment of vendor products and services.” The language in the order does not match the language in the standard and therefore suggest that the language be consistent to provide clarity.

15) There could be an impact of contract requirements on the ability of public utilities to piggyback on wide-area contracts such as those of National Association of State Procurement Officials (NASPO) Cooperative, Western States Contracting Alliance (WSCA), Washington State Department of Enterprise Service, and others. Recommend that an exclusion be permitted in the case of such contracts, which are important to provide flexibility, effectiveness, and negotiating strength for public utilities throughout the country. In some cases such contracts are required; also include language that provides an exclusion for contracts that are covered by other laws or regulations.

16) The measure should not reference the word mitigation, which to an auditor may limit the actions an entity might take to address risk (such as avoid or transfer). Suggest that “mitigate” be replace with “address” as listed in R1.2.

Likes 1	Austin Energy, 3, Preston W. Dwayne
Dislikes 0	

Response	
Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	
Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No
Document Name	
Comment	
The FERC order applied to industrial control systems. The SDT is applying the standard to all BES Cyber Assets or systems. It is our belief that all BES Cyber systems are not industrial control systems. The SDT should apply the requirements to industrial control systems such as DCS or EMS systems located in power plants and control rooms.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Colorado Springs Utilities (CSU) has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.	

CSU does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CSU requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CSU believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CSU requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CSU requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CSU is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as national, regional, state & city negotiated contracts. Examples include contracts from the National Association of State Procurement Officials (NASPO) Cooperative and the Western States Contracting Alliance. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they provide important negotiating strength, flexibility, and effectiveness in contracting (see CS's Uresponse to Question #9 for additional information on exceptions).

CSU notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CSU requests changing the word *evaluate* to *determine.*

For R1.2.1 CSU requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CSU requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CSU requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

In Measure M1, CSU requests that the language be changed to be consistent with the Requirement. Specifically, change “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…” to “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…” (BOLD emphasis added). The construction “address risk” conforms with the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as opposed to mitigated.

CSU requests that the title of the standard be changed to “Vendor Risk Management” to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term “supply chain risk management” encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013

address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

The Rationale for R1 states, “Implementation of elements contained in the entity’s plan related to Party 1.2 is accomplished through the entities procurement and negotiation process.” The SDT need to define the process for determining the minimum level deemed to be sufficient. Additionally, the SDT needs to identify the course of action an entity must take and document where a vendor is unwilling or unable to meet the obligations set forth for Responsible Entities.

R1. In FERC Order No. 829, paragraph 59 states, “The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.” The Order does not address requirements for EACMS, PACS, or PCA as identified in R1. The SDT should limit the requirement to the context of the Order.

R1.1.1. The obligation to “identify and assess risks” is extremely open-ended and ambiguous. In contrast, the draft Technical Guidance and Examples document enumerates a list of 11 factors that should be considered in an entity’s plan. NERC standards should be clear on their face, and it is inappropriate to require and entity to refer to draft Technical Guidance and Examples document for fundamental questions concerning whether an entity is compliant with a given requirement. If the Drafting Team believes that this list of 11 factors within the draft Technical Guidance and Examples document is a comprehensive list of factors that should be considered when “identifying and assessing risks,” these factors should be listed in the standard as the exhaustive set of factors to be assessed. If the Drafting Team does not believe this list is complete or appropriate, an alternate list of factors should be provided. Without clear requirements on the factors to be considered, there is substantial risk in inconsistency of implementation by entities.

R1.1.1. The use of the term “deployment” can be read to require an ongoing obligation even after the software or hardware is in production. To avoid confusion, the term “deployment” should be removed.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	CIP-013 Comment Mar 2 revision SCL 2017-3-6.docx

Comment

The attached document has comments compiled for all the questions. Please note that the BOLD paragraphs below (YELLOW highlighted in attachment) are uniquely Seattle City Lights. The un-highlighted comments were developed in collaboration with other entities and trade organizations such as LPPC. These comments may be like those submitted by other entities but not necessarily. City Light recognizes the challenges facing the SDT and appreciates the efforts the SDT is placing into working towards developing a solid standard.

Seattle City Light has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

Seattle City Light does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, Seattle City Light requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, Seattle City Light believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, Seattle City Light requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

Seattle City Light requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

Seattle City Light is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as national, regional, state & city negotiated contracts. Examples include contracts from the National Association of State Procurement Officials (NASPO) Cooperative and the Western States Contracting Alliance. In some cases use of these contracts in procurement is mandated by other laws or regulations. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they provide important negotiating strength, flexibility, and effectiveness in contracting (see Seattle City Light’s response to Question #9 for additional information on exceptions).

Seattle City Light notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 Seattle City Light requests changing the word *evaluate* to *determine.*

For R1.2.1 Seattle City Light requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 Seattle City Light requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. Seattle City Light requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

In Measure M1, Seattle City Light requests that the language be changed to be consistent with the Requirement. Specifically, change “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…” to “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…”

(BOLD emphasis added). The construction "address risk" conforms with the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as alternatives to being mitigated.

Seattle City Light requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.

Likes 0	
Dislikes 0	

Response

Linda Jacobson-Quinn - City of Farmington - 3

Answer	No
Document Name	

Comment

FEUS supports the comments submitted by APPA

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA agrees with comments submitted by American Public Power Association.

Likes 0	
Dislikes 0	

Response

Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	

It is unclear how the risk and requirements in R5 for Low Impact BES Cyber Systems are differentiated from the other requirements and how the requirements will be measured considering a list of Low Impact systems are not required. There seems to be some reduncancy between R1 and R5 for Low Impact. Suggest removing Low Impact requirements from CIP-013 and incorporating into CIP-003 for consitency.

Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	

Ambiguity in R1

FERC Order No. 829 asks for a plan to be developed and implemented by the entity that **includes** security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. It recognizes the diversity of BES Cyber System environments, technologies and risks among entities. FERC states that the “Reliability Standard may allow a responsible entity to meet the security objectives discussed below by having a plan to apply different controls based on the criticality of different assets.”

We find that the use of word “address” in R1 is creating ambiguity.

We suggest that requirement should be clear in stating that entities are to identify supply chain cyber security risks, evaluate controls and select controls, and implement controls based on their acceptable risk levels for future procurement contracts.

In doing so, entities should consider, at minimum, the controls that are itemized in the FERC Order and evaluate whether implementation of those controls are appropriate based on risk.

The four objectives that R1 should address are not clear

FERC Order states the “following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., the Reliability Standard should set goals (the “what”), while allowing flexibility in how a responsible entity subject to the Reliability Standard achieves that goal (the “how”)).”

The required plan is not tied to the objectives stated in the FERC Order.

1. For Information System Planning, FERC Order appears to ask that the responsible entity must include security considerations as part of its information system planning and system development lifecycle. The information system planning and development lifecycle should be periodically reviewed and approved by CIP Senior Manager.

We believe that R1.1 is intended to address the Information System Planning objective in the FERC Order. Consideration of security risks in Information System Planning is the objective of the overall plan.

R1.1 causes ambiguity. It is not clear how controls can be used to identify and assess risk. Controls are used to mitigate risk. Evaluation of controls is performed prior to their selection depending on the acceptable level of risk and cost associated with the controls. The verbiage of Part 1.1.2 requires controls for the evaluation of methods to address risks. It does not require risks to actually be determined.

2. R1.2 lists a number of controls (some specifically stated in the FERC Order) and does not identify which objective these controls are to address.

a. For Software Integrity and Authenticity objective, FERC Order appears to ask that at minimum, entities should consider implementing the following controls to mitigate risk by:

1. Verifying the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; and

2. Verifying the integrity of the software and patches before they are installed in the BES Cyber System environment. (R1.2.5)

The Standard appears to address this objective in Requirement 3. There is overlap/redundancy between R1.2.5 and Requirement 3.

b. For Vendor Remote Access to BES Cyber Systems, FERC Order appears to ask that at minimum, entities should consider implementing controls to mitigate risk by Logging and controlling all third-party (i.e., vendor) initiated remote access sessions including user-initiated and machine-to-machine vendor remote access. (R1.2.6)

The Standard appears to address this objective in Requirement 4. There is overlap/ redundancy between R1.2.6 and Requirement 4.

c. For Vendor Risk Management and Procurement Controls, FERC Order appears to ask that at minimum, entities' controls should consider implementing controls to mitigate by means of:

1. Vendor security event notification processes; (R1.2.1)

2. Vendor personnel termination notification for employees with access to remote and onsite systems; (R1.2.2)

3. Product/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords; (R1.2.3)

4. Coordinated incident response activities; and (R1.2.4)

5. Other related aspects of procurement. (R1.2.7)

Related to R1.2.1, It is not clear what constitutes a "vendor security event". Every vendor may have a different consideration for what constitutes a "security event". It could include an instance of employee fraud, workplace assault, or even the announcement of a patch release.

Related to R1.2.4, Cyber Security Incident is a NERC defined term. Is a cyber security incident a Cyber Security Incident? If not, what is the distinction? If it is, the term will need to be capitalized. Also the term "vendor related cyber security incident" is not clear. Is it a Cyber Security Incident that could happen during procurement and deployment stage?

We also find R1.2.7 is unnecessary and creates ambiguity.

Applicability

FERC Order suggests that entities can perform their own assessment of risks and determine applicability of controls based on that.

It is not clear how the described controls are applicable to BES Cyber Systems based on their risk level in the context of CIP Standards (Low, Medium, and High).

The Standard extends applicability to the EACMS, PACS, and PCAs associated to BES Cyber Systems. We argue that PACS, EACMS and PCAs, although are important for Physical and Electronic Security, are not necessarily “industrial control system hardware, software, and computing and networking services associated with bulk electric system operations” as stated in the FERC Order.

This standard should not be applied to systems or assets not needed for BES operations.

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment

The NYPA Comments

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

Sacramento Municipal Utility District (SMUD) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

SMUD does not agree with including all BES Cyber Systems in Requirement R1. SMUD supports a risk-based approach, while limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, SMUD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, SMUD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

SMUD requests that the SDT add the following language from the rationale to the language of the standard: "Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts."

SMUD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see SMUD's response to Question #9 for additional information on exceptions).

SMUD notes that the Rationale for R1 includes a definition of the term "vendors". This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 SMUD requests changing the word *evaluate* to *determine.*

For R1.2.1 SMUD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 SMUD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. SMUD requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Requirement Placement (CIP-013 versus CIP-003)

R1 (and R2) includes low, medium, and high BES Cyber Systems; however, the current CIP Standards put the low impact BES Cyber Systems (LIBCS) requirements in CIP-003. EEI recommends that the SDT consider whether to move the LIBCS requirements from CIP-013 into CIP-003. Moving the LIBCS to CIP-003 may make it easier for Responsible Entities with only LIBCS to implement the requirements.

However, Responsible Entities with high, medium, and low impact BES Cyber Systems (HIBCS, MIBCS, and LIBCS) may be concerned that moving the supply chain LIBCS requirements to CIP-003 may make it difficult for them to take a holistic approach to the CIP-013 requirements. For example, some entities may want to focus on their BES Cyber System vendors and apply a single vendor-based approach for HIBCS, MIBCS, and LIBCS. Also, CIP-013 is focused on the risk that vendors and suppliers may introduce into BES Cyber Systems, whereas the other CIP Standards are focused on more general cybersecurity risks that can be addressed by Responsible Entity operational controls, which are within the control of the Responsible Entity. Third-party risk is harder for Responsible Entities to control and the methods of control are more likely contractual than operational. For example, a Responsible Entity cannot control a vendor's manufacturing process, but can ask questions during procurement as to how security risk is managed by the vendor to help evaluate the level of risk the vendor may pose to the Responsible Entity. As a result, there may be value in keeping these requirements out of the other CIP Standards, which focus on operational controls for cybersecurity risk.

Applicable Systems

Requirement R1 applies to LIBCS as well as HIBCS and MIBCS and their associated EACMS, PACS, and PCAs. We do not believe that EACMS, PACS, and PCAs should be included under the scope of Requirement R1. The diversity and sheer number of these systems make it difficult to document how Responsible Entities will address procurement for all of these systems in their risk management plans. Auditing these plans will also be difficult.

Some products and services may pose greater risk than others depending on many factors including risk introduced by the vendor, risk introduced by the vendor's product/service, or how the Responsible Entity deploys the vendor product or service. As a result, the requirement's objective should be to get Responsible Entities to evaluate vendor cybersecurity practices during procurement and develop methods to mitigate potential risks, whether that is choosing another vendor, implementing an operational control, or accepting the risk. CIP-013 cannot address all risk introduced by vendors and their products and services. Vendors have a responsibility to reduce risk in their manufacturing processes and Responsible Entities have a responsibility to reduce risk in their operations. The existing CIP standards already address Responsible Entity operational risk.

We are also concerned that by specifying the applicable systems in Requirement R1 that the requirement may be interpreted that every device in a system must be addressed by these plans. We recommend that the SDT consider either narrowing the scope of the requirement language or making it more flexible to allow Responsible Entities to define which systems need to be addressed by the plans based on the risk. For example, using "industrial control systems associated with BES Cyber Systems" may narrow the scope to more critical systems; however, industrial control systems would need to be defined by the SDT as interpretations may vary.

Security Objective

The security objective of Requirement R1 is unclear. Although it focuses on the Commission objectives 3 and 4, it would be helpful to make it clear in the requirement language so that Responsible Entities understand the purpose of the requirement.

Objective 3 is focused on making sure that Responsible Entities do not unintentionally plan to procure or fail to anticipate security issues during procurement or technology/vendor transitions. Objective 4 is focused on ensuring security concepts are addressed in future contracts. Both of these objectives are focused on evaluation of the risk that the vendor or vendor product/service may introduce to the BCS by the Responsible Entity during planning for and actual procurement of new systems. The controls that are required under Requirement R1 are also not operational controls, but process controls to assess and evaluate the risk.

Risk Acceptance

We understand that Order No. 706 ordered the ERO to remove acceptance of risk language from the CIP Reliability Standards. In this case, it was tied to a concern over uncontrolled compliance exceptions to addressing potential vulnerabilities and the Commission preferred the use of technical feasibility, which led to technical feasibility exceptions. (See Order No. 706, P 150-151) We are not recommending the use of "acceptance of risk" in CIP-013, but we want to make it clear that risk acceptance may be a good option in dealing with procurement controls (CIP-013, Requirement R1), which are different than the operational controls covered by the other CIP Standards.

The security objective for Requirement 1 is focused on Responsible Entity awareness of risk that may be introduced by the vendor or vendor product/service. The Responsible Entity's ability to control this risk is limited. For example, the Responsible Entity may only have a few vendors to choose from for a particular procurement and the vendors may not have a well-defined process for vendor security event notification. The Responsible Entity can ask them to define a process and can even put language into a contract to require such a contract, but the vendors can say no. The Responsible Entity is left with the choice of either not procuring this device or system or accepting the risk. Documenting a compliance exception for every term the vendor does not agree to does not seem reasonable in light of the scope of Requirement R1 – the sheer numbers of systems covered (HIBCS, MIBCS, and LIBCS) and diversity of vendors for each of these systems and system components. Responsible Entities also cannot make the vendor develop or follow this process even if the vendor agrees to, which is also a consideration for the SDT – if the vendor does not comply with their contract terms is the Responsible Entity subject to a violation and penalty?

We recommend that the SDT consider, set, and articulate compliance expectations with Requirements R1 and R2 and recognize the difference between these procurement controls and the operational controls found in the rest of the CIP Standards.

Measure M1

We are concerned with the M1 language use of "written agreements" as a measure of plan implementation, even though it is introduced with "could include, but is not limited to." Requirement R1 does not (and should not) require Responsible Entities to use contract terms to meet the security objective. However, contract terms may be one method of "how" to meet the security objective ("what"), but not all entities will choose this "how". We are concerned that the inclusion of "written agreements" in the measure text suggests that this is a key piece of evidence for compliance with R1. Also, the use of "correspondence" in M1 could include "written agreements" if an entity chooses to use them for R1. We recommend removing "written agreements in electronic or hard copy format" from M1.

We recommend the following language for consideration by the SDT:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) to minimize the cyber security risks from vendors and vendor products and services to BES Cyber Systems during planning and procurement of industrial control systems. The plan(s) should address one or more methods to:

1.1. Raise awareness of risk the vendor and vendor product or service may introduce, including awareness of vendor process(es) to:

1.1.1. Notify the Responsible Entity of vendor security events;

1.1.2. Notify the Responsible Entity of when vendor employee remote or onsite access should no longer be granted;

1.1.3. Disclose known vulnerabilities to the Responsible Entity;

1.1.4. Coordinate the response to vendor-related cyber security incidents with the Responsible Entity;

1.1.5. Verify the software integrity and authenticity of vendor software and patches; and

1.1.6. Control remote access, including vendor-initiated interactive remote access and system-to-system remote access to the Responsible Entity

1.2. Assess risk(s) introduced by the vendor and vendor product or service identified by Part 1.1; and

1.3. Evaluate method(s) to address risk(s) identified by Part 1.2.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language. Particularly R1 should only focus on supply chain risk management during the procurement phase rather than controls during operations. Operational controls on BES systems should be covered in other CIP standards. Furthermore, if controls are to be required on a vendor's manufacturing process, in addition to those identified during RFP negotiations, these controls should be consistent and verifiable by an industry standard (similar to ISO(?) 9001 certification).	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, LCRA requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, LCRA believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, LCRA requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.	
Likes 0	
Dislikes 0	
Response	

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

Many of the aspects of CIP-013-1 R1 cannot be controlled by the entity, but instead need to have assurances from the vendor. In other CIP standards there are operational controls that the entity can make to meet the requirements of the standards; these controls are things the entity can control.

The scope of R1 includes BCAs, EACMS PACS and PCAs with no guidance concerning the risk associated with each of these types of assets. Some products and services may pose greater risk than others depending on many factors including risk introduced by the vendor, risk introduced by the vendor's product/service, or how the Responsible Entity deploys the vendor product or service. As a result, the requirement's objective should be to get Responsible Entities to evaluate vendor cybersecurity practices during procurement and develop methods to mitigate potential risks, whether that is choosing another vendor, implementing an operational control, or accepting the risk. CIP-013 cannot address all risk introduced by vendors and their products and services. Vendors have a responsibility to reduce risk in their manufacturing processes and Responsible Entities have a responsibility to reduce risk in their operations. The existing CIP standards already address Responsible Entity operational risk.

We are also concerned that by specifying the applicable systems in Requirement R1 that the requirement may be interpreted that every device in a system must be addressed by these plans. We recommend that the SDT consider either narrowing the scope of the requirement language or making it more flexible to allow Responsible Entities to define which systems need to be addressed by the plans based on the risk. For example, using "industrial control systems associated with BES Cyber Systems" may narrow the scope to more critical systems; however, industrial control systems would need to be defined by the SDT as interpretations may vary.

Likes 0	
Dislikes 0	
Response	

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	No
Document Name	
Comment	

The IRC and SWG thanks the Drafting Team for their work and support the concepts in the security program enhancements addressing supply chain risks.

The Rationale for R1 states, "Implementation of elements contained in the entity's plan related to Party 1.2 is accomplished through the entities procurement and negotiation process." The SDT need to define the process for determining the minimum level deemed to be sufficient. Additionally, the SDT needs to identify the course of action an entity must take and document where a vendor is unwilling or unable to meet the obligations set forth for Responsible Entities.

R1. In FERC Order No. 829, paragraph 59 states, “The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.” The Order does not address requirements for EACMS, PACS, or PCA as identified in R1. The SDT should limit the requirement to the context of the Order.

R1.1.1. The obligation to “identify and assess risks” is extremely open-ended and ambiguous. In contrast, the draft Technical Guidance and Examples document enumerates a list of 11 factors that should be considered in an entity’s plan. NERC standards should be clear on their face, and it is inappropriate to require and entity to refer to draft Technical Guidance and Examples document for fundamental questions concerning whether an entity is compliant with a given requirement. If the Drafting Team believes that this list of 11 factors within the draft Technical Guidance and Examples document is a comprehensive list of factors that should be considered when “identifying and assessing risks,” these factors should be listed in the standard as the exhaustive set of factors to be assessed. If the Drafting Team does not believe this list is complete or appropriate, an alternate list of factors should be provided. Without clear requirements on the factors to be considered, there is substantial risk in inconsistency of implementation by entities.

R1.1.1. The use of the term “deployment” can be read to require an ongoing obligation even after the software or hardware is in production. To avoid confusion, the term “deployment” should be removed.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Many of the aspects of CIP-013-1 R1 cannot be controlled by the entity, but instead need to have assurances from the vendor. In other CIP standards there are operational controls that the entity can make to meet the requirements of the standards; these controls are things the entity can control.

The scope of R1 includes BCAs, EACMS PACS and PCAs with no guidance concerning the risk associated with each of these types of assets. Some products and services may pose greater risk than others depending on many factors including risk introduced by the vendor, risk introduced by the vendor’s product/service, or how the Responsible Entity deploys the vendor product or service. As a result, the requirement’s objective should be to get Responsible Entities to evaluate vendor cybersecurity practices during procurement and develop methods to mitigate potential risks, whether that is choosing another vendor, implementing an operational control, or accepting the risk. CIP-013 cannot address all risk introduced by vendors and their products and services. Vendors have a responsibility to reduce risk in their manufacturing processes and Responsible Entities have a responsibility to reduce risk in their operations. The existing CIP standards already address Responsible Entity operational risk.

We are also concerned that by specifying the applicable systems in Requirement R1 that the requirement may be interpreted that every device in a system must be addressed by these plans. We recommend that the SDT consider either narrowing the scope of the requirement language or making it more flexible to allow Responsible Entities to define which systems need to be addressed by the plans based on the risk. For example, using “industrial control systems associated with BES Cyber Systems” may narrow the scope to more critical systems; however, industrial control systems would need to be defined by the SDT as interpretations may vary.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

Q1-Issue1-Discussion

(1) In reviewing the measures M1, R1 is written in a manner to collect evidence to achieve two objectives; (i) documentation of the plan, and (ii) documentation to demonstrate implementation of the plan(s). According to NERC's Drafting Team Reference Manual which was recently revised and published October 19, 2016, on page 11 under section B – Requirements and Measures (http://www.nerc.com/pa/Stand/Resources/Documents/Drafting%20Team%20Reference%20Manual_Oct2016_final.pdf), each requirement should "achieve one objective." The Reference Manual goes on to state: *If a requirement achieves two objectives, such as developing a document and distributing that document, then each objective should be addressed in its own requirement.* Contrary to instructions delineated in the Reference Manual, R1 requires Entities meet two objectives, develop **and** implement the supply chain risk management plan.

Q1-Issue1-Recommendation

GTC recommends R1 be separated into two separate requirements where the first objective of the FERC directive identified in paragraph 2 is addressed to "develop a plan" (R1), and the second objective is addressed in its own requirement to "implement the plan" (new R2). This method simplifies compliance documentation for the Responsible Entity and aligns with the principles documented in NERC's Reference Manual. Additionally, this method will simplify and provide clarity to achieve FERCs directive for the plan to be forward-looking as explained in further detail below.

Q1-Issue2-DISCUSSION

(2) The SDT has clarified in the rationale for requirement R1 that the implementation of the cyber security risk management plans(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 as specified in the Implementation Plan. Additionally, Paragraph 59 stipulates to address security concepts in "future contracts". However, GTC does not see this forward looking language in the actual Requirement R1 that is specified by the FERC Order. GTC believes this forward looking language can be better clarified and highlighted if the SDT accepts GTC's first recommendation to separate R1 into two requirements and "implement the plan" is written as its own requirement.

Q1-Issue2-Recommendation

GTC recommends the following:

Separate R# to implement plan(s), then update the new Requirement with the following language: "Each Responsible Entity shall implement the documented supply chain risk management plan(s) specified in Requirement R1. Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts."

Q1-Issue3-DISCUSSION

(3) Paragraph 45 of Order No. 829, clearly specifies “The Plan” should address, at a minimum, four specific security objectives in the context of addressing supply chain management risks.

(P. 45) The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

Although R1 technically covers the four specific security objectives, the presentation lends itself somewhat confusing. R1.2.5 seems to align with security objective (1), R1.2.6 seems to align with security objective (2), and are both subsets to R1.2 which seems to align with security objective (4).

Q1-Issue3-Recommendation

GTC believes R1 will be clearer to understand and that the drafting team could gain more support if the four specific security objectives required by Order 829 Paragraph 45 had their own individual sub-requirement of “The Plan”, in lieu of sub-requirements of one of the security objectives such as:

R1.1 aligns with security objective 3 (*information system planning*) where the specifics of the third objective identified in paragraph 56 is captured as a subset of R1.1;

R1.2 aligns with security objective 4 (*vendor risk management and procurement controls*) where the specifics of the fourth objective identified in paragraph 59 is captured as a subset of R1.2;

R1.3 to align with security objective 1 (*software integrity and authenticity*) where the specifics of the first objective identified in paragraph 48 is captured as a subset of R1.3; and

R1.4 to align with security objective 2 (*vendor remote access*) where the specifics of the second objective identified in paragraph 51 is captured as a subset of R1.4.

Q1-Issue4-DISCUSSION

(4) Order 829 Paragraph 58 refers to NIST Special Publication 800-53 for various supply chain development life cycle controls. The definition of Supply Chain from NIST SP 800-53 r4 states that the “supply chain horizon" ends at the delivery of products/services to the acquirer. FERC Order 829 acknowledges this definition in paragraph 32, footnote 61.

Supply Chain: “Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer”

Accordingly, in the system lifecycle, the supply chain management process occurs prior to the identification of a Cyber Asset as a BES Cyber System pursuant to the implementation of CIP-002-5.1a. This designation must only occur “upon commissioning” for planned system installations (and even later for unplanned changes). Therefore, BES Cyber System identification, categorization as high, medium, or low impact; and also identifying associated EACMS, PACS, and PCAs does not exist during the supply chain context. Therefore, R1 should be limited to a supply chain risk management plan which will address controls for mitigating Supply Chain risks to hardware, software, and computing and networking services of Cyber Assets which are intended to support Bulk Electric System operations as specified in Order 829 paragraph 43.

Q1-Issue4-Recommendation

GTC recommends the SDT adopt the aforementioned NIST SP 800-53 defined term Supply Chain for use with CIP-013-1 R1 in front of the term “risks” to contain the Time Horizon to supply chain risk management, and also edit to account for the fact that BES Cyber System identification and categorizations do not exist during the supply chain context.

An example of R1 is provided:

R1. Each Responsible Entity shall document a Supply Chain risk management plan(s) that address controls for mitigating Supply Chain risks to hardware, software, and computing and networking services which are intended to support Bulk Electric System operations. The plan(s) shall address:

R1.1 The use of controls for mitigating Supply Chain risks associated with *information system planning*

R1.2 The use of controls for mitigating Supply Chain risks associated with *vendor risk management and procurement controls*

R1.3 The use of controls for mitigating Supply Chain risks associated with *software integrity and authenticity*

R1.4 The use of controls for mitigating Supply Chain risks associated with *vendor remote access*

Q1-Issue5-DISCUSSION

GTC disagrees with the inclusion of associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets in requirement R1. GTC finds no reference to the inclusion of these associated systems in FERC Order 829 and recommends their removal from this standard.

Further, GTC questions whether the use of the term BES Cyber Systems is appropriate in a standard which is limited per FERC Order 829 to “the context of addressing supply chain management risks.” In the system lifecycle, the supply chain management process occurs prior to the identification of a Cyber Asset as a BES Cyber System pursuant to the implementation of CIP-002-5.1a. This designation must only occur “upon commissioning” for planned system installations (and even later for unplanned changes). Therefore, BES Cyber System identification, categorization as high, medium, or low impact; and also identifying associated EACMS, PACS, and PCAs does not exist during the supply chain context.

Q1-Issue5-Recommendation

GTC recommends the removal of any reference to Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. GTC recommends removal of references to BES Cyber Systems and replacing it with the phrase “hardware, software, and computing and networking services which are intended to support Bulk Electric System operations.”

Likes 0	
Dislikes 0	

Response

Bob Case - Black Hills Corporation - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

R1.1 is acceptable in regard to requiring entities to have a plan to identify and assess risks with procured equipment. R1.2 is unacceptable because Entity creation of Detective Controls for the four Objectives of P. 45 is considered out of the Entity's scope. If only one Entity and one Vendor existed, the individual sub-parts of R1.2 may be feasible for control planning – but this approach is not viable for hundreds of entities and dozens of vendors. The Entity is capable of identifying Preventative Controls, in concept, but they will only be effective if all the vendors in the supply chain make a diligent effort to implement the controls all the way back to the first-line suppliers. Corrective Action Controls are critical, but would be able to be implemented only after a problem is identified.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich

Answer	No
Document Name	

Comment

See comments submitted by Black Hills Corporation

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
The requirement should focus on the risk of the software or services being procured and not allow for the possibility of a Registered Entity taking a risk view based upon the impact categorization of the BES Cyber System or EACMS, PACS, or PCA that is affected by the procurement. The requirement needs to clearly be focused on the vendor processes without regard to the Cyber Assets impacted by the vendor. The controls need to include processes for granting vendor access in addition to the processes for notifying when removal of access is necessary. The controls to grant access should include expectations for the conduct of training and personnel risk assessments, including review, modification as necessary, and acceptance of the vendor's process by the Registered Entity, if applicable, along with expectations of what evidence of compliance will be provided to the Registered Entity by the vendor. Part 1.2.4 should include an expectation of notification by the vendor in addition to coordination of the response.	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	
1) The Rational for Requirement R1 includes a definition of the term "vendors". This definition is also included in the Guidelines and Examples document. This term should be officially defined.	

2) It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.

3) R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:

“The entity must document its determination as to what are the supply chain risks. Once this determination has been made and documented, the audit team’s professional judgement cannot override the determination made by the Responsible Entity. “

For R1: With respect to the obligation to “identify and assess risks,” the standard is extremely open-ended. In contrast, the Compliance Guidance enumerates a list of 11 factors that should be considered. NERC standards should be clear on their face, and it should not be necessary to refer to Compliance Guidance for basic questions concerning whether an entity is in compliance with a given requirement. If the Drafting Team believes that this list of 11 factors is a comprehensive list of factors that should be considered when “identifying and assessing risks,” these factors should be listed in the standard as the exhaustive set of factors to be assessed. If the Drafting Team does not believe this list is complete or appropriate, a complete list of factors should be provided. Without clear guidance, as to factors that should be considered, there is substantial compliance risk if a subjective auditor disagrees with the risk factors identified by an entity

R 1.1.1 – The use of the term “deployment” can be read to require an ongoing obligation even after the software or hardware is in production (i.e. once deployed). To avoid confusion, the term “deployment” should be removed or clarified.

4) For R1: This requirement requires both the development and the implementation of a plan. Recommend breaking this into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement plan in future contracts.

5) For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” This should be incorporated into the Requirement itself.

6) For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list “planning, acquisition and deployment” and versions of these terms in the diagram. R1.1 uses “planning and development”. The meaning of “development” has not been clarified and is not part of the process addressed by this standard. Suggest that “development” be clarified or removed.

7) For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

a. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

b. To evaluate the effectiveness of mitigating that risk? or;

c. Is it meant to identify the controls in place to mitigate the identified risks?

8) For R1.2.1: The words “Security Event” are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then” Security Event” should be replaced or clarified in the Requirement. This clarification could include “any identified, threatened, attempted or successful breach of the vendor’s components, software or systems used in the support of the Entity’s BES Cyber System.” This new language differentiates R1.2.1 from the vulnerabilities in R1.2.3

9) For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.

10) For R1.2.2: The requirement for the” process for notification” is very different than the “request vendor cooperation” guidance given on page 6, line 22 of the guidance document the requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that “A failure of a vendor to follow a defined process is not a violation of this Requirement.”

For R1.2: A newly added (in the 1/19/17 draft) sentence in the Rationale (R1) section states: “Implementation of elements contained in the entity’s plan related to Part 1.2 *is accomplished* through the entities procurement and negotiation process. Who determines whether it was a sufficient effort to “implement the elements” as part of the procurement and negotiation process? What if you take their first “no” for an answer – is that sufficient effort to implement? Who gets the final sign off?

11) Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk?

The Compliance Guidance states: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.” What qualifies as an *existing contract*? Is there an obligation to implement the risk management plan when: (1) negotiating and executing a new Statement of Work; (2) negotiating an amendment to a Master Agreement; or (3) renewing a contract under existing terms? The answer to these questions should be clarified and directly addressed in the standard.

Requirements overlap with existing CIP standards and create double jeopardy situations. Change 1.2.7 from pointing to 1.1.2 to 1.1.1

The following statements from the R1 Rationale box are important caveats for compliance and should be included in the Requirement text:

“Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

“Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”

Likes 0	
Dislikes 0	

Response

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	

Comment

- What is meant by “if applicable” in the Requirement. If this means EACMS/PACS/PCAs for high and medium impact BES Cyber Systems, then state this.
- Extending the applicability to all BES Cyber Systems and associated EACMS/PACS/PCAs results in an unfathomable expansion in scope. For example, in a small Medium Impact Control Center BES Cyber System, we have between 50 and 60 individual software and hardware contracts to manage. Most common industry practices would base the procurement policies for these contracts based on their financial risk, or contracts above a certain spending threshold. However, managing cyber risk does not relate to spending. A million-dollar EMS system could carry less cyber security risk than a $20 camera or a one thousand-dollar network switch. This implies a centralized procurement office for all purchases, since each potential purchase needs to be evaluated for the Cyber Security risk it presents. This would have tremendous costs for smaller entities. We suggest limiting the scope to high and medium impact BES Cyber Systems.
- 1.2.3 should read “known [security] vulnerabilities”. Vulnerabilities include any weakness in the code.
- What does coordination mean in 1.2.4 and 1.2.6?
- Remove 1.2.7. This does not belong in a mandatory and enforceable Standard. As it stands, an entity is required to add other indeterminate processes.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	

Comment

See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
R1.1 is acceptable in regard to entities having a plan to identify and assess risks with procured equipment. R1.2 is unacceptable because the entity creation of Detective Controls for the four Objectives of P. 45 is considered out of the Entity's scope. If only one Entity and one Vendor existed, the individual sub-parts of R1.2 would be feasible for a control plan – but this approach is not viable for hundreds of Entities and dozens of vendors. The Entity is capable of identifying Preventative Controls, in concept, but they will only be effective if the vendors in the supply chain make a diligent effort to implement the controls to the first-line suppliers. Corrective Action Controls are critical, but would be able to be implemented only after a problem is identified. Corrective Action Controls are critical, but would be able to be implemented only after a problem is identified.	
Likes 0	
Dislikes 0	
Response	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Response	

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
FERC didn't specifically ask for Low Impact BES Cyber Systems to be included but didn't explicitly exclude them either. SunPower does not believe Low Impact Cyber Systems should have to meet the same expectations of High and Medium Impact Cyber Systems. While we appreciate the efforts of the SDT to meet the expectations of the FERC Order, we believe the SDT may have gone beyond what FERC was asking them to do. CIP-003-6 does not require Entities with Low Impact Cyber Systems to have to list the BES Cyber Systems, with this new requirement, do Entities lose their exception? If there is an expectation of that Low Impact Cyber System Entities must adhere to the same or lesser requirements as High and	

Medium Impact Cyber System Entities, then perhaps CIP-003 would be a better place for the exception. SunPower believes CIP-013, as written, is in direct conflict with the intent of CIP-003-6.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 1. In addition, we offer the following comments: **Remove Identify, Assess, and Control Found at the Requirement Level** We suggest deletion of these words and terms. The use of identify, assess, and control (IAC) is represented by the responsible entity's governance and control structure. This is an evaluation performed by the Regional Entity in evaluation of the responsible entity's inherent risk and oversight model.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
Oxy disagrees that R1 should be applicable to low impact BES Cyber Systems. Although FERC is silent on whether low impact should be included, Paragraph 2 of Order No. 829 says "nor does the Commission require NERC to propose "one-size-fits-all" requirements. The new or modified Reliability Standard should instead require responsible entities to develop a plan to meet the four objectives, or some equally efficient and effective means to meet these objectives, while providing flexibility to responsible entities as to how to meet those objectives." The language of R1 elevates low impact BES Cyber Systems to the level of medium and high impact BES Cyber Systems. For example, R 1.2.2 requires a process for when vendor employee remote or onsite access should no longer be granted. Under existing CIP Standards, Access Management Program requirements reside in CIP-004 and none are applicable to low impact BES Cyber Systems. R 1.2.5 requires processes for verifying software integrity and authenticity of all software and patches that are intended for use. Under existing CIP Standards, Security Patch Management requirements reside in CIP-007 and none are applicable to low impact BES Cyber Systems. Additionally, software and patching typically occurs at the Cyber Asset level and low impact entities are only required to identify assets containing low impact BES Cyber Systems. As currently written, R1 and its sub-requirements seem to require an inventory of Cyber Assets or BES Cyber Systems, neither of which are required of low impact entities, which is another element that elevates low's to	

that of medium and high. Using a risk based approach, it seems more appropriate that R1 be applicable to medium impact and high impact only. The risk assessments are required and performed under CIP-002 and the determination made that low impact BES Cyber Systems pose a minimal threat to the BES. Finally, under the existing CIP suite of standards, requirements applicable to low impact entities reside in CIP-003. If a risk management plan is to be required, low impact with a reduced set of requirements to address their minimal BES risk, Oxy requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5. Oxy also requests that CIP-013-1, R1 be rewritten to be applicable to medium and high impact BES Cyber Systems only.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	No
Document Name	

Comment

- Regarding R1.2.1, vendors will unlikely to share security events. Registered Entities should not be held accountable for compliance obligations in which they have no control of.
- Regarding R1.2.1, the Standard Drafting Team should clarify what is intended by, “vendor security event.” This is an ambiguous term which can have different meanings.
- Regarding R1.2.3, the Standard Drafting Team should clarify what is intended by, “known vulnerabilities.” This is an ambiguous term which can have different meanings.
- Regarding R1.2.4, the Standard Drafting Team should clarify what is intended by, “cyber security incidents.” This is an ambiguous term which can have different meanings.
- Regarding R1.2.4, vendors will be unlikely to share cyber security incidents. Registered Entities should not be held accountable for compliance obligations in which they have no control of.
- Regarding R1.2.5, this requirement is duplicative of CIP-007-6. The Standard Drafting Team should clarify how proposed requirement would be completed within the Procurement phase.
- Regarding R1.2.6, this Requirement is duplicative of CIP-005-5.

.

Likes 0	
Dislikes 0	

Response

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No

Document Name	
Comment	

The scope of the requirement is not clear due to the phrase "if applicable." Please clarify how an entity would determine if their Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets are applicable.

Due to some vendors offering many of their products and services outside of the electric utility industry (Microsoft, Cisco, Symantec, GE…) there is a concern that entities will lack leverage when negotiating these new terms and will likely find it difficult to come to an agreement. There are also instances where there are very few options available to industry for a particular product, device, or service. Does the SDT envision that registered entities would be forced to find alternative vendors or products if they are unable to come to an agreement?

It is not clear if the requirements are only applicable to new software purchases or also apply to upgrades of existing software (including adding additional licenses for existing software) or renewals of software maintenance contracts that provide software upgrades of existing software. If the existing software is already in place, there is concern that there will be the lack of leverage to require vendors of existing software to negotiate new terms.

Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	

Concur with EEI’s Position

Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	

SVP agrees with other entity comments to limit this requirement to High and Medium only, as current low impact requirements does not require entities to conduct an inventory of equipment and software or identify systems. Pleas also see APPA's comments, with which SVP is in agreement.

Likes 0	

Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	

Comment
The need for such a broad set of requirements is unnecessary due to the existing CIP requirements for the entity to have an incident response plan, anti-virus protection and patch management. To the extent the following items remain in R1, NRECA proposes the following actions: R1.2 – Recommend deleting text after “BES Cyber Systems” as the text is unnecessary. R1.1.1 – Clarify what is meant by “vendor security events.” R1.2.3 – What is the basis for determining what are “known vulnerabilities?” R1.2.4 – Clarify the scope of this language as it seems unnecessarily open-ended. R1.2.5 – Clarify that this item is for BES Cyber Systems only. R1.2.7 – Delete as it is unclear and unnecessarily open-ended.

Likes 0	
Dislikes 0	

Response

Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	

Comment
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements; however, EPE would like to emphasis one issue that is at the forefront of its concerns: The proposed language of the requirements (especially Requirement 1.2) speaks in terms of using controls that “address process(es),” and yet, the contents of the requirements include “verifying software integrity.” Responsible Entities are familiar with various existing CIP requirements that mandate the development of “processes,” but in CIP-013-1, the inclusion of responsibility for verifying software integrity places a Responsible Entity in a conundrum not present in the other Reliability Standards. Must a Responsible Entity start hiring employees with software capabilities equal or better than the software developers on the staff of the vendors who have historically supplied software products to the industry? If so, how long will that take

and at what cost to ratepayers, and can a third party effectively or efficiently create a pool of talent superior to the actual developers of the vendor's software itself?

Perhaps there is room in the standard for a Responsible Entity to simply require in its processes that any vendor will provide an attestation to the Responsible Entity that the vendor's software product is authentic and has integrity for the intended use, making this type of attestation a means of complying with the verification requirements found throughout CIP-013-1 in its proposed form. If so, the current wording of the draft standard does not plainly or clearly say so.

EPE understands the objective of the standard, and the Commission's desire to tackle the risks that stem from third party vendors whose work may impact the BES. Our participation in the balloting process for this standard is with the goal of arriving at language that is clear and that enables a Responsible Entity to comply.

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements; however, EPE would like to emphasis one issue that is at the forefront of its concerns:

The proposed language of the requirements (especially Requirement 1.2) speaks in terms of using controls that "address process(es)," and yet, the contents of the requirements include "verifying software integrity." Responsible Entities are familiar with various existing CIP requirements that mandate the development of "processes," but in CIP-013-1, the inclusion of responsibility for verifying software integrity places a Responsible Entity in a conundrum not present in the other Reliability Standards. Must a Responsible Entity start hiring employees with software capabilities equal or better than the software developers on the staff of the vendors who have historically supplied software products to the industry? If so, how long will that take and at what cost to ratepayers, and can a third party effectively or efficiently create a pool of talent superior to the actual developers of the vendor's software itself?

Perhaps there is room in the standard for a Responsible Entity to simply require in its processes that any vendor will provide an attestation to the Responsible Entity that the vendor's software product is authentic and has integrity for the intended use, making this type of attestation a means of complying with the verification requirements found throughout CIP-013-1 in its proposed form. If so, the current wording of the draft standard does not plainly or clearly say so.

EPE understands the objective of the standard, and the Commission's desire to tackle the risks that stem from third party vendors whose work may impact the BES. Our participation in the balloting process for this standard is with the goal of arriving at language that is clear and that enables a Responsible Entity to comply.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No
Document Name	
Comment	

The applicability of this requirement should be limited to high and medium impact BES Cyber Systems. Low impact Cyber Systems are categorized as low impact because they inherently have a low ability to negatively impact the Bulk Electric System. We should focus our resources on those systems that have the potential for significant adverse impact on the BES. We can re-evaluate at a later date whether additional requirements should be established for low impact BES Cyber Systems.

Using “if applicable” adds confusion to the language. If it is not always applicable to associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets, define where it is applicable and where it is not.

We’re concerned that the word “Evaluate” in requirement 1.1.2 might imply that all possible methods for addressing the risks will need to be evaluated. We prefer replacing the term “Evaluate” with “Identify”. Additionally, there may be occasion where a risk is identified but is judged to be at an acceptable level given the ability or inability to address it. This standard, in its entirety, should be about minimizing the risks and/or providing reasonable assurance which may result in some instances where the entity will accept a certain level of risk as reasonable. Therefore, we propose the following language: 1.1.2. Identify methods to address the above risk(s), as needed.

Requirement 1.2.1 requires “Process(es) for notification of vendor security events”. CIP-007-6 R4 Security Event Monitoring includes a requirement for generating alerts for security events. Assuming that Requirement R1.2.1. is intended to mean the entity will have a process to encourage and direct vendor notification to the client, we suggest this be included in the language of CIP-007.

Requirement 1.2.2 requires “Process(es) for notification when vendor employee remote or onsite access should no longer be granted” The revocation of access, including Interactive Remote Access is currently addressed in CIP-004-6 R5. If this is attempting to require something above and beyond those requirements, it should be made clear what that is and consideration given to housing all of these requirements in CIP-004.

Requirement 1.2.3 requires “Process(es) for disclosure of known vulnerabilities”. Is this asking for entities to have a process for the entity to disclose vulnerabilities? Who would we be disclosing to? If it’s directed at vendors, the entity can discuss this with the vendor, but the vendor is under no obligation to disclose vulnerabilities and neither the entity, nor FERC, has the authority to require this. Vendors MAY disclose vulnerabilities, but that will likely occur concurrent with providing a fix/patch.

Requirement 1.2.4 requires a “Coordination of response to vendor-related cyber security incidents”. From our understanding of what this requires, we believe this is already covered in the entities cyber security incident response plan (CIP-008).

Requirement 1.2.7 requires “Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable”. While we understand what this requirement is intending to do, we believe it is may lead to second-guessing by auditors and/or unrealistic auditor expectations.

Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements; however, EPE would like to emphasis one issue that is at the forefront of its concerns:

The proposed language of the requirements (especially Requirement 1.2) speaks in terms of using controls that "address process(es)," and yet, the contents of the requirements include "verifying software integrity." Responsible Entities are familiar with various existing CIP requirements that mandate the development of "processes," but in CIP-013-1, the inclusion of responsibility for verifying software integrity places a Responsible Entity in a conundrum not present in the other Reliability Standards. Must a Responsible Entity start hiring employees with software capabilities equal or better than the software developers on the staff of the vendors who have historically supplied software products to the industry? If so, how long will that take and at what cost to ratepayers, and can a third party effectively or efficiently create a pool of talent superior to the actual developers of the vendor's software itself?

Perhaps there is room in the standard for a Responsible Entity to simply require in its processes that any vendor will provide an attestation to the Responsible Entity that the vendor's software product is authentic and has integrity for the intended use, making this type of attestation a means of complying with the verification requirements found throughout CIP-013-1 in its proposed form. If so, the current wording of the draft standard does not plainly or clearly say so.

EPE understands the objective of the standard, and the Commission's desire to tackle the risks that stem from third party vendors whose work may impact the BES. Our participation in the balloting process for this standard is with the goal of arriving at language that is clear and that enables a Responsible Entity to comply.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	Final_Unofficial_Comment_Form_2016-03_03162017_ERCOT comments.docx

Comment

ERCOT supports the IRC comments and offers the following supplemental comments.

FERC Order 829, Paragraph 59, states that NERC's new or modified standard "must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations." This does not include the Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs) listed in R1. These systems do not perform or provide bulk electric system operations. ERCOT believes the inclusion of these systems in the draft standard goes beyond the scope of the standard intended by FERC and recommends the SDT remove them from the applicable systems of the standard language.

Requirement R1 requires Responsible Entities to have a plan that addresses processes for notification of a vendor's cyber security events (R1.2.1) and vulnerabilities (R1.2.3), as well as coordination of cyber security incident response activities (R1.2.4). As this information is highly sensitive, it is unlikely that all vendors will agree in all cases to provide this information unless they are already required to do so under other regulatory obligations. Responsible Entities cannot force a vendor to agree to these terms, and in cases where the vendor deems the risk of this disclosure too great compared to the value of the contract, the vendor will decline to enter into the agreement. This will force the Responsible Entity to seek another vendor that is

willing to accept these terms, and such a vendor may or may not exist. Because it is possible that a Responsible Entity may be unable to identify a vendor that is willing to accept a contract with the terms required by R1, the proposed standard could seriously hamper the essential functions of Responsible Entities. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R1. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

Requirement R1.2.2 requires "notification when vendor employee remote or onsite access should no longer be granted." The revocation of access, including Interactive Remote Access, is currently addressed in CIP-004, R5. Since the background checks, training, access authorization, and access revocation for employees and vendors is already addressed in CIP-004, the drafting team should ensure any new requirements related to access revocation of vendors be placed in CIP-004. In developing the CIP Version 5 standards, extensive work was undertaken to ensure that all requirements related to the subject were included in one standard instead of being spread across multiple standards. The proposed language will disrupt that framework.

Requirement R1.2.5, which requires a Responsible Entity's plan to include "Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use," is duplicative of Requirements R3 and R5 within this standard, which also require documentation of processes. ERCOT recommends removing R1.2.5.

Requirement R1.2.6 requires an entity's plan to include "Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)." This requirement is duplicative of Requirement 4 within this standard. ERCOT recommends removing Requirement R1.2.6, which also requires documentation of processes.

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	Yes

Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Requirement R1 states “supply chain risk management plan(s)” while M1, R2, M2 states “supply chain cyber security risk management plan(s)”. ReliabilityFirst recommends the SDT use consistent language so that there is no confusion on terminology.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
While in overall agreement with Requirement 1, ACEC does have the following concerns: 1. Part 1.1 requires the Responsible Entity to identify and assess risk(s) and evaluate methods to address identified risks. This requirement specifically changes the methodology for risk assessment defined in CIP-002-5.1. As noted in the Background section (Section 6) of the standard, "This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards." This view of risk based upon the impact of BES Cyber Assets based upon the impact to the BES, not the devices cyber security risk, was defended by NERC and approved by FERC in Order 791 approving Version 5 of the CIP Standards. Based upon this, it would be consistent with CIP-002-5.1 to remove Part 1.1 of Requirement 1, modify requirement R1, Part 1.2.7 to state "other process(es) to address risk(s) as determined in CIP-002-5.1 R1, Parts 1.1 and 1.2" and to add to requirement R1 that it only applies to high and medium impact BES Cyber Systems as used in R3 and R4. 2. In the Rationale for Requirement R1, the term vendor is defined as "(i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators." ACEC is concerned that by including product resellers or vendors, who have no direct or indirect control of these areas, misapplication of the procurement language in this Standard would impose unrealistic obligations, standards of care, and potential liability on professional services related to the supply chain. As a consequence, services currently provided by	

engineering firms may be uninsurable under current professional liability insurance policies. Other industries supporting the supply chain have raised similar concerns, noting that the effect of this approach will be to stifle competition, impair innovation, and increase costs.

Specifically, the guidance language in this Standard includes "integrator" requirements that impose responsibilities on engineering firms and other supply chain elements for control of software development; personnel management systems; industrial system controls (SCADA); and long- term or post-contract reporting/remediation requirements (vulnerability testing and mitigation). Engineering firms do not typically develop such software and hardware, yet the guidance language suggests they should assume such liability for their use. They also do not monitor and report vulnerabilities for vendor software and hardware. This "one-size-fits-all" approach amounts to a significant reallocation of risk, imposing liability on engineering firms that they can neither manage, nor price. The result will be fewer firms willing to perform services for this industry. This requirement should be modified to limit the scope and responsibilities to the vendor and end user to ensure risk is apportioned to the responsible parties.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	

Comment

Requirement R1 requires a documented ‘supply chain risk management plan’, AZPS requests clarification and renaming of the plan to ‘vendor risk management plan’ throughout the Standard as this term more appropriately describes the content that is required to be included in the plan. Also, the statement …’the plan(s) shall address:’ seems redundant and potentially creates a distinction that is not intended. AZPS recommends striking the last sentence and appending …’including’ to the first sentence of Requirement R1. Finally, AZPS recommends revising the language of Requirement R1 to focus on BES Cyber Systems and to allow the plan content to address when the associated “Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets” are brought into the scope of such plans as follows:

R1. Each Responsible Entity shall implement one or more documented ***Vendor*** risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems, ***including***: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. The use of controls in BES Cyber System planning and development to:

1.1.1. Identify and assess risk(s) during the procurement and deployment of vendor products and services; and

1.1.2. Evaluate methods to address identified risk(s).

1.2. The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems:

1.2.1. Process(es) for notification of vendor security events;

1.2.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.2.3. Process(es) for disclosure of known vulnerabilities;

1.2.4. Coordination of response to vendor-related cyber security incidents;

1.2.5. Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

1.2.6. Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and

1.2.7. Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.

1.3. The applicability of controls to associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

AZPS also requests that two (2) definitions utilized in the Technical Guidance and Examples be proposed for inclusion as defined terms in the standard, "Security Events" and "Vendor." Specifically, AZPS notes that Requirement R1.2.1 uses the term "security events" as an undefined term in the Standard, but that the Technical Guidance and Examples, Page 6, uses "Security Events" as a defined term. AZPS requests consistency between the two documents and the addition of the defined term "Security Events" to the Standard. Additionally, AZPS requests the removal of 'identified, threatened, attempted' from the defined term and require only notification of 'successful breach of vendor's components, software or systems that have potential adverse impacts to the availability or reliability of BES Cyber Systems'. Further, the Rationale for Requirement R1 defines the term "vendors" as '(i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators', AZPS requests incorporating this definition in the Standard for specificity of scope.

AZPS requests clarification regarding the term "processes" as used in Requirement R1.2. In particular, AZPS requests clarification that these items or "processes" are to be included in the overall plan and do not require a separate process or process documentation. Finally, the Rationale for Requirement R1 states that "obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement the Entity's plan;" however the Requirement does not make clear that the failure of contract negotiations to result in specific controls would not be considered a failure to implement.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

PSEG agrees with the intent of this requirement, but has the following questions/recommendations below:

- The term vendors as used in the standards is defined in the Rationale for Requirement R1 box. This term should be officially defined in the Glossary of Terms used in NERC Reliability Standards.

- Is requirement R1 applicable to new additions and/or modifications to existing BES Cyber Systems? There is not sufficient information to determine if this requirement is applicable only to new BES Cyber Systems or if it also includes changes to existing BES Cyber Systems.

- The applicability of Requirement R1 to High/Medium/Low BES Cyber systems and EACMs, PACs and PCAs is not clear the way it is written. Recommend using the applicability tables as in CIP-004 through CIP-011 for the requirements in this standard, especially R1.

- Requirements 1.2.1 through 1.2.6 discuss processes for vendor controls but some of the controls are unclear as to who is expected to perform the “notification”. For each sub-requirement, PSEG recommends adding clarity in the requirement language indicating who is expected to perform the notification, the vendor or the registered entity.

- Requirement 1.2.1 discusses a vendor security event. This is a vague term. The standard should include more clarification on what a vendor security event is or define the term.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company strongly encourages the SDT to consider the below edits, which use phrasing directly from the FERC Order. If R1 is intended to address the true supply chain procurement side of things, then the proposed edits provided below appropriately scope this requirement at the ‘main R’ level. The Order 829 Summary, and paragraphs 10 and 24 of the Order specify controls for vendors that supply “industrial control systems” products and services. Therefore, R1 should be focused on to what vendors and what software/firmware this requirement should be limited. The expansion of scope at this stage to propose including all impact classifications of BES Cyber Systems and their associated EACMS, PACS, and PCAs is above and beyond the Order, in our opinion. It’s absolutely unmanageable if not restricted somehow to higher level systems. In CIP audits, “BES Cyber Systems” immediately turn into a list of hundreds or thousands of "programmable electronic devices."

The proposed edits provided below move the “planning and procurement” phases of the lifecycle up from sub-requirements 1.1 and 1.1.1 to the main requirement so that all of the sub-requirements under R1 are appropriately scoped as well. Without this, for example, R1.2 applies to all risks at all times throughout the entire lifecycle of all devices. It’s cleaner to have the ‘main R’ be about the plan and setting the scope of the plan, and then have the sub-requirements address the plan(s) specifics. Consistent with Order 829, language from the rationale section addressing the “forward-looking” nature of this new requirement(s) has been incorporated into the main R1 requirement itself. Modifications highlighted below in R1.2.5 are recommended to eliminate redundancy and avoid confusion, while also addressing the specifics in the Order for dealing with “cyber incidents.” The order of the sub-requirements of R1.2 have also been adjusted to more clearly align with the planning and procurement life-cycle, while at the same time continuing to address directives in the Order.

Additionally, Southern Company agrees with comments submitted by Georgia Transmission Corporation (GTC), specifically with regard to defining the term “Supply Chain” in accordance with the Order-referenced NIST 800-53 defined term which establishes the applicable time horizon for this Standard, and removal of references to Electronic Access Control and Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

Modify the R1 language as follows:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating planning and procurement cyber security risks for industrial control system vendor products and services used in BES Cyber Systems. Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts. The plan(s) shall address: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Process(es) for the identification and assessment of risk(s) *of industrial control system vendor products and services*.

1.2 Methods to evaluate controls to address identified risk(s) in R1.1, that includes the following:

1.2.1 Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s);

1.2.2 Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.2.3 Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

1.2.4 Process(es) for disclosure of known vulnerabilities in vendor products;

1.2.5 Process(es) for notification of and coordination of response to vendor-related cyber security incidents; and

1.2.6 Other process(es) to address risk(s) as determined in Part 1.1, if applicable.

Likes 0	
Dislikes 0	

Response

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	

Jeanie Doty - Austin Energy - 5	
Answer	
Document Name	
Comment	
For all Questions - I support the comments of Andrew Gallo, Austin Energy	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
The draft Requirement R1.2 language creates compliance concerns due to the need for Responsible Entities to negotiate commercial contracts with vendors that commit the vendors to undertake the tasks necessary for R1.2, particularly in circumstances where only a single vendor has the capability of providing the necessary services for Cyber Assets covered by CIP-013-1. For example, unless a vendor agrees to notify the Responsible Entity of vendor-identified vulnerabilities in the Cyber Assets provided or maintained by the vendor, Responsible Entities cannot comply with R1.2.3. Responsible Entities could encounter scenarios where: • Vendors may refuse to comply with the Responsible Entity’s vendor controls; • Vendors may demand an unreasonably high payment for compliance with the Responsible Entity’s vendor controls; • Vendors may agree to Responsible Entity controls but fail to take the steps necessary to implement those controls in a compliant manner; or	

• Software/firmware made by a vendor no longer in business and unable to assist the Responsible Entity in the integrity and authenticity verification process.

To ensure that compliance with CIP-013-1 does not place Responsible Entities in an untenable negotiating position, a compliance “safety valve” is necessary to allow Responsible Entities to comply with the Standard even in the absence of vendor assent to the Responsible Entity’s required controls. Such a “safety valve” would be consistent with the current draft guidance on CIP-013-1 R1.2, which states that “[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan.”

Guidance language in the G&TB portion of a Standard is helpful, but the “safety valve” concept should be included within the language of the Requirement itself because only that language forms the basis of a compliance assessment.

Exelon has sent ideas under separate cover to the Drafting Team Chair outlining three options for providing the necessary “safety valve” along with proposed text edits to the requirements. In short, these options include a technical feasibility exception, a commercial feasibility exception or a simple exception documentation process.

Likes 0	
Dislikes 0	

Response

Devin Elverdi - Colorado Springs Utilities - 1

Answer	
Document Name	

Comment

Refer to CSU comments.

Likes 0	
Dislikes 0	

Response

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

The Rational for Requirement R2 lists several sources for supply chain vulnerabilities, but it is not clear what is considered a relevant source and whether the entity is required to review all sources of supply chain vulnerabilities which may be very burdensome. CenterPoint Energy recommends adding the specific sources of vulnerability information, such as E-ISAC or ICS-CERT in the requirement.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	

Comment

1) Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.

2) For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.

3) Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

1. Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.
2. For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.
3. Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

4. SDT should clarify that existing contracts do not need to be renegotiated based on the 15-calendar month reassessment of the plan or other plan revisions.

5. Will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? Seems to imply scope creep from elements on R1. Is *necessity* in R1 defined by entity, NERC, or outside source?

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG recommends that each requirement should have a provision for allows an entity to accept the risk of selection a vendor that will not or cannot supply a control. NRG recommends removal of R2.1 language which is covered in R2.

For R2, will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? This seems to imply scope creep from elements on R1. Is “necessity” defined by entity, NERC, or outside source?

NRG requests clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

- Dominion recommends that requirement R2 be replaced with the following:

“Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 related to procuring and installing unsecure equipment or software, the risk of unintentionally failing to anticipate security issues that may arise due to network architecture, unintentionally arise during technology and vendor transitions, and purchasing software that is counterfeit or that has been modified by an unauthorized party at least once every 15 calendar months, which shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]”*

Dominion is of the opinion that the activities specified in Part 2.1 are included in the language of R2. Dominion recommends modifying Part 2.1 and 2.2 as follows:

- 2.1 Revision(s), if any, to address applicable new supply chain security risks that include security considerations related to cyber security, and
- 2.2 The supply chain plan(s) shall be reviewed, updated as necessary, and approved by CIP SM or delegate at least once every fifteen (15) months.

Also see the recommendation for replacing this requirement as described in the comments for R1.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

Refer to our comments on R1.

We do not agree with the approach in R1 (and R2) of creating “plans” and the intent of the plans to “cover the procurement aspects of all four objectives.”

Order 829’s four objectives did not include creating “plans.” All four of the directives either direct or use examples of specific operational cyber security controls which are best addressed as revisions to CIP-002 through -011.

NERC’s Compliance Registry Summary of Unique Entities and Functions as of March 3, 2017, identifies 1,398 unique NERC entities. These entities range from entities with a couple breakers for low impact Facilities (lines), to entities operating gigawatts of low impact generation units to entities operating high-impact Control Centers for thousands of miles of medium impact Transmission Facilities, for example. All have BES Cyber Assets.

With respect to R2 as proposed, 1,398 entities would have to annually research information, including information which is readily available to be proactively provided by NERC to them. This diverts and dilutes registered entities’ resources.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response
Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

Exelon feels that the R2.1 language is vague and has the potential to become administratively burdensome without a corresponding benefit to BES reliability. While Exelon agrees with the rationale that examples of sources of information that an entity could consider include guidance or information issued by the E-ISAC, this language should be included in the Requirement itself because only that language forms the basis of a compliance assessment. Exelon receives over 100 security-related messages regarding potential vulnerabilities per day from a myriad of sources. Without creating bounds around the sources to be considered as well as the periodicity for updates to supply chain cyber security risk management plan(s), the question of whether any or all of the messages should have been considered will be difficult, if not impossible, to evidence. Exelon points out that the E-ISAC already performs important filtering functions for the industry. Perhaps future Alerts issued by the E-ISAC could be enhanced to point out vulnerabilities that would require new mitigating controls in supply chain cyber security risk management plan(s). Without these limitations, each entity will need to develop processes and procedures to receive and filter information, define mitigating controls, update the plan(s) and obtain approvals which is inefficient at best and impossible to evidence at worst.

Further, Exelon suggests that while multiple updates to the plan(s) may occur within a year as new E-ISAC Alerts are issued, CIP Senior Manager Review and Approval should only be required every 15 months. Intermediate reviews and approvals, or reviews for minor changes, should be outside the scope of the Requirement.

Likes 0	
Dislikes 0	

Response
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

We suggest moving this Requirement language to the CIP-003 Standard. Our group feels that CIP-003 is the most appropriate Standard to handle this Requirement which is applicable to Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response
Nicholas Lauriat - Network and Security Technologies - 1

Answer	No

Document Name	
Comment	
Approval of CIP Senior Manager or delegate should be required for both or neither of R1 and R2.	
Likes 0	
Dislikes 0	
Response	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx
Comment	
See comments on Requirement R2 in attached file.	
Likes 0	
Dislikes 0	
Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	No
Document Name	
Comment	

Basin Electric would prefer low impact requirements be included in CIP-003 rather than CIP-013.

The language of R2.1 appears redundant and not any different than what is already required in the language of the main requirement, R2. Suggest deleting R2.1.

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1

Answer	No
Document Name	

Comment

Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4

Answer	No
Document Name	

Comment
• As previously stated, for consistency with other CIP Standards (e.g. Physical Security plans, Incident Response Plan, Recovery Plans, Information Protection program, etc..) , CIP-003 R1.1 should be expanded to include the Supply Chain Risk Management plan as part of the collective cyber security policies reviewed and approved by the CIP Sr. Manager at least every 15 months. And, applicability of supply chain risk management controls to assets that contain Low Impact BCS should be consigned to CIP-003, R1.2 and R2. • The NERC Glossary of Terms definition of CIP Senior Manager will require update to include CIP-013

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	

Comment
We agree with the LPPC/APPA comments.

Likes 0	
Dislikes 0	

Response

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment
R2 contains the language “As necessary… at least once every 15 months…” Is it an “as necessary” requirement or is it once per 15 months? Recommend removing the “as necessary” language as it is too subjective and open to interpretation.

Likes 0	
Dislikes 0	

Response

W. Dwayne Preston - Austin Energy - 3

Answer	No

Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

1. Suggest deleting R2.1. The R2 language includes “review and update as necessary”. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.
2. For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.
3. Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

Likes 0	
Dislikes 0	
Response	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	

Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI supports the following comment from AEP: “R2 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R2 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R2 should be rewritten to be only applicable to high and medium impact BES Cyber Systems.”	
Likes 0	
Dislikes 0	
Response	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
R2 has no stated applicability and it is unclear whether the CIP Senior Manager approval required here is any different from the required approval under R5. It would be clearer if R2 were made into R1.3, with the clarification suggested in our comments above to clearly exclude Low BES Cyber Assets from this requirement and consolidate requirements for those assets under R5.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
What is the target of the word “revisions” at the beginning of R2.1? Does revisions refer to modifications of the “supply chain cyber security risk management plan(s)” document itself? If so, then requirement is redundant in that R2, and consequently R2.1 could be interpreted to require entities to evaluate the revisions that were just completed. Or is the intent of “revisions” to direct REs to consult document(s) external to the standard when executing revisions?	
Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.	

Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
R2 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R2 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R2 should be be rewritten to be only applicable to high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	

The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Luis Rodriguez - El Paso Electric Company - 6

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

R2 – first line – for clarity purposes NRECA recommends removing “and update, as necessary.”

R2.1 – strongly recommend deleting “to address applicable new supply chain security risks and mitigation measures” as it is unclear and unnecessarily open-ended.

Likes 0	
Dislikes 0	

Response

Val Ridad - Silicon Valley Power - 1 - WECC

Answer	No
Document Name	

Comment

SVP agrees with other entity comments that "additional evaluation of the revisions is an administrative task that does not enhance BES security."

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Concur with EEI’s Position	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
For consistency with other CIP Standards, CIP-003 R1.1 should be expanded to include supply chain risk management as part of the collective cyber security policies to be reviewed and approved by the CIP Sr. Manager at least every 15 months and removed from CIP-013-1.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute’s comments to Question 2.	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	

The way the Requirement is written once again leaves the Requirement open to interpretation.

The current text reads:

“Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, which shall include:”

SunPower believes the correct statement of R2 should read:

“Each Responsible Entity shall review, as necessary, but at least once every 15 calendar months, its supply chain cyber security risk management plan(s) specified in Requirement R1 and update as necessary. The reviews and updates includes, but not limited to:”

SunPower also believes that the intent of R2.1 is not clear when the Requirement states, “to address applicable new . . . “ SunPower believes the term “applicable” needs to be left out of the Requirement unless the SDT is talking to the Applicability Section of the Standard, if that is the case, then state the Applicability Section. If that is not the case, SunPower believes the sub part should read:

“2.1 Evaluation of revisions, if any to address newly identified supply chain security risks and mitigation measures”

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

We generally agree with EEI’s comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

Agree that it is appropriate to reassess the Entity plan associated with R1.1, but updates to the R1.2 portion would be unmanageable to point of being non-productive for entities and suppliers, for the reasons already stated in the R1 response above.

Likes 0	
Dislikes 0	
Response	
George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	
Comment	
See Black Hills Corp comments	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	
Comment	
The annual assessment of new risk is too open ended for a mandatory and enforceable Standard.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	
1) Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.	

2) For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.

3) Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

SDT should clarify that existing contracts do not need to be renegotiated based on the 15-calendar month reassessment of the plan or other plan revisions.

Will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? Seems to imply scope creep from elements on R1. Is *necessity* in R1 defined by entity, NERC, or outside source?

Likes 0	
Dislikes 0	

Response

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick

Answer	No
Document Name	

Comment

Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

It is not clear if the approval by the CIP Senior Manager is required with the first version of the plans, or only for subsequent revisions. It is not clear if the approval by the CIP Senior Manager or delegate is required with each review cycle or only if modifications are made to the document(s).

Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Agree that it is appropriate to reassess the Entity plan associated with R1.1. For the reasons already stated in the R1 response, updates to the R1.2 requirements would be unmanageable to point of being non-productive for entities and suppliers.	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC knows of no definitive source to identify “new supply chain security risks and mitigation measures.” Therefore, compliance with this requirement part becomes subjective thus is not auditable. Reviewing and updating the plan as necessary under the core R2 along with CIP Senior Manager approval per R2.2 should be sufficient to maintaining a quality cyber security supply chain risk management program. We recommend the removal of requirement part 2.1.	

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

The rationale for Requirement R2 suggests that every Responsible Entity should assess all supply chain risks before updating the plan, which may be a very burdensome requirement that will be difficult to comply with and audit. Would a Responsible Entity be in violation if it didn't document that they read a particular DHS report? Also, the Requirement R1 plan is focused on methods to review, assess, and evaluate vendor and vendor product/service risk before entering into a contract with a vendor, these methods are unlikely to change all that much based on guidance issued by NERC or DHS and would be naturally covered by a periodic review and approval of the plan(s).

Also, part 2.1 requires an evaluation of revisions to address new supply chain security risks and mitigation measures. It is unclear how a revision to address a new supply chain security risk is different than a mitigation measure. A mitigation measure addresses a risk.

We recommend the following language for consideration by the SDT:

R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

We feel that there should be some guidance on where to look for "emerging supply chain related concerns". If our company is using a particular source and miss a notification on another site, will we be penalized?

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No
Document Name	

Comment

With regards to the periodic reassessment of supply chain cyber security risk management controls, the IRC and SWG request the SDT provide objective criteria for the scope and content of the review to ensure consistent implementation against set criteria. Does this only require update of the plan document? Do needed contract revisions have to be documented? What is required to demonstrate review and consideration of items that may not be incorporated into the updated plan?

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

The rationale for Requirement R2 suggests that every Responsible Entity should assess all supply chain risks before updating the plan, which may be a very burdensome requirement that will be difficult to comply with and audit. Would a Responsible Entity be in violation if it didn't document that they read a particular DHS report? Also, the Requirement R1 plan is focused on methods to review, assess, and evaluate vendor and vendor product/service risk before entering into a contract with a vendor, these methods are unlikely to change all that much based on guidance issued by NERC or DHS and would be naturally covered by a periodic review and approval of the plan(s).

Also, part 2.1 requires an evaluation of revisions to address new supply chain security risks and mitigation measures. It is unclear how a revision to address a new supply chain security risk is different than a mitigation measure. A mitigation measure addresses a risk.

We recommend the following language for consideration by the SDT:

R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

We feel that there should be some guidance on where to look for "emerging supply chain related concerns". If our company is using a particular source and miss a notification on another site, will we be penalized?

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC

Answer	No
Document Name	

Comment

SDG&E agrees with EEI comments and proposed language. R2 needs a more clear description on when mitigation measures are required. For example, would the selection of one vendor over another be considered a mitigation measure? Would an entity be required to always choose the vendor with the best-in-class security posture despite cost?

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

The rationale for Requirement R2 suggests that every Responsible Entity should assess all supply chain risks before updating the plan, which may be a very burdensome requirement that will be difficult to comply with and audit. Would a Responsible Entity be in violation if it didn't document that they read a particular DHS report? Also, the Requirement R1 plan is focused on methods to review, assess, and evaluate vendor and vendor product/service risk before entering into a contract with a vendor, these methods are unlikely to change all that much based on guidance issued by NERC or DHS and would be naturally covered by a periodic review and approval of the plan(s).

Also, part 2.1 requires an evaluation of revisions to address new supply chain security risks and mitigation measures. It is unclear how a revision to address a new supply chain security risk is different than a mitigation measure. A mitigation measure addresses a risk.

We recommend the following language for consideration by the SDT:

R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment

The NYPA Comments

Likes 0	
Dislikes 0	

Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
We believe that sub requirements (2.1 and 2.2) in R2 are unnecessary. Similar verbiage used in CIP-003-6 for review of cyber security policy can be used in this instance. Also, can the CIP Senior Manager delegate this accountability?	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	

Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment
With regards to the periodic reassessment of supply chain cyber security risk management controls, the IESO request the SDT provide objective criteria for the scope and content of the review to ensure consistent implementation against set criteria. Does this only require update of the plan document? Do needed ntract revisions have to be documented? What is required to demonstrate review and consideration of items that may not be incorporated into the updated plan?

Likes 0	
Dislikes 0	

Response

Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No
Document Name	

Comment
This should be removed and convered in CIP-003.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	

Comment
1) Suggest deleting R2.1. The R2 language includes “review and update as necessary”. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.

Likes 0	

Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
BPA believes if the scope and language for R1 is appropriate, the review process is necessary but should not require CIP Senior Manager Approval. BPA suggests maintaining consistency across standards: CIP Senior Manager approval is required for policies rather than plans.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
R2 IPC suggests the SDT consider re-structuring the proposed format for R2 to align with current enforceable standard format (see CIP-002-5.1 R2, R2.1, and R2.2): The Responsible Entity shall: (1) Review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, (2) Evaluate revisions, if any, to address applicable new supply chain security risks and mitigation measures; and (Question) How does the SDT foresee this evaluation being measured and accomplished? (3) Obtain its CIP Senior Manager or delegate approval (Question) Is the CIP Senior Manager or delegate intended to be an approval of the plan every 15 months? If so, IPC recommends specifying the timing and what is being approved in the wording of the requirement. IPC does not believe R2.2 provides any security measures or controls and is simply an administrative exercise. IPC recommends R2.2 be removed.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	
Comment	

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016.

Reclamation recommends Requirement R2 should instead require entities to implement their supply chain risk management plan(s) developed in Requirement R1.

Within each Requirement, the sub-requirements should distinguish between high, medium, and low impact BES Cyber Systems and other supporting systems. Reclamation recommends the implementation plan enforcement dates be staggered based on high, medium, and low impact for auditing purposes and to allow the associated risks and severity levels to be spelled out more clearly.

Likes 0	
Dislikes 0	
Response	

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE

Answer	No
Document Name	
Comment	

1. Requiring a greater level of testing, documentation, or security features from system integrators, suppliers, and external service providers may increase the price of a product or service, and increase the compliance burden for the industry. We recommend language addressing key questions, such as: at what time frame does the risk reduce to acceptable: Daily, weekly, monthly or yearly? How is the standard addressing acceptance of risk?

Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli

Answer	No
Document Name	
Comment	

Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Brian Bartos - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

While it is not unreasonable to propose periodic review and reassessment to assure some minimum level of rigor, ultimately Registered Entities know that plans are living documents that must be supported by sound security practices implemented to stay apprised of emerging cybersecurity threats as they enter the landscape, and a 15-month reassessment is ill-equipped to support the pace of the ever-evolving threat landscape. The industry might be better served with language that supports a periodic review coupled with the need for ongoing and timely assessment and update of plans on an as needed basis when the impending threat warrants the action.

The SDT may want to reconsider the need and intended value for CIP Senior Manager approval for these reasons. 1.) While it is not unreasonable to propose an approval for plans of this nature, prescribing this as a CIP Senior Manager responsibility is inconsistent with other enforceable mandatory CIP Cyber Security Reliability Standards that limit these approvals to BES Cyber System populations, policy, and, exceptions (both CIP Exceptional Circumstances and Technical Feasibility Exceptions). 2.) The introduction of CIP Senior Manager or delegate approval may not provide the intended value for the complex range of jurisdictional, technical, economic, and business relationship issues. 3.) By NERC definition, as a technicality, please note that the scope of the CIP Senior Manager accountabilities is currently prescribed as CIP-002 – CIP-011 and would require amendment. 4.) Lastly, as a consideration, the SDT may want to revisit the need for this level of approval and to align the approach with the former efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate requirements are administrative in nature only and therefore that do not provide security or reliability value.

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	

1. Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.

1. For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.

Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

SDT should clarify that existing contracts do not need to be renegotiated based on the 15 calendar month reassessment of the plan or other plan revisions.

An entity’s plan must be implemented at the commencement of negotiations.

Will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? Seems to imply scope creep from elements on R1. Is *necessity* in R1 defined by entity, NERC, or outside source?

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	

Comment

R2 is pretty straightforward, however unless modified by a subsequent implementation plan, WECC would expect an entity to have a reviewed and approved SCRM plan on or before the effective date, then complete R2 on intervals of no more than 15 calendar months. If an entity exceeds the 15 calendar month time frame, an R2 PNC would be indicated.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment
SRP agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, SRP requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes
Document Name	

Comment
CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Likes 0	
Dislikes 0	

Response

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
While supporting this requirement, ACEC recommends that the requirement be modified to state it only applies to high and medium impact, consistent with requirements R3 and R4.

Likes 0	

Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	

AE agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, AE requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	Yes
Document Name	

Comment

PRPA agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, PRPA requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3

Answer	Yes
Document Name	

Comment

CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	Yes
Document Name	
Comment	

Duke Energy suggests the drafting team consider collapsing 2.1 and 2.2 into one sub-requirement. We do not see the need in having these as two sub-requirements, and this would mirror the language used in CIP-003-6.

Also, the use of the term “applicable” in R2.1, appears vague and could lead to potential disagreement on what supply chain security issues actually pose a substantial risk.

Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	Yes
Document Name	
Comment	

Proposed CIP-013-1, R2 properly implements Order No. 829’s directive to develop a Standard requiring entities to periodically review and approve the controls adopted to address specific security objectives associated with supply chain risk management.

Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	
Comment	

No additional comments.

Likes 0	
Dislikes 0	
Response	

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The use of 15 calendar months allows entities to review and update (as required) on a systematic basis, the same time every year, Thank you.	
Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern Company strongly encourages the SDT to consider the below edits to R2 to make it clear that assessment of risks and revisions to the plan are required on a “once every 15 months” interval, and not at the time of each and every notification of any new potential risks/vulnerability. The below proposed modifications also clarify that *revisions* to the plan(s) are predicated on the existence of “new supply chain cyber security risks” by moving the phrase “if any.” Subsequently, R2.2 has been modified to require CIP Senior Manager or delegate approval only when, following a required review every 15 months, it is determined revisions to the plan(s) are warranted to address “new supply chain cyber security risks” or “mitigation measures.” As written in the draft Standard, an annual review and approval by the CIP Senior Manager or delegate where no revisions were warranted or made is a documentation exercise that provides no benefit to reliability or reduction of supply chain risk. The SDT should also consider strengthening the language in the Rationale and/or Guidelines directing Entities to adequate and/or designated sources (NERC/DHS/E-ISAC/ICS-CERT) providing Supply Chain guidance for those higher level issues that warrant a change to your plan(s). Also of note and for SDT consideration is the structure of the Implementation Plan for this Standard that does not require the CIP Senior Manager or delegate to review and approve the initial plan(s) on or before the effective date the plan(s) is required to be in place; therefore, review and approval of the plan(s) would be 15 months after the plan(s) was already in effect.

Modify R2 language as follows:

R2. Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in Requirement R1 and update them, as necessary, at least once every 15 calendar months, which shall include:

2.1. Evaluation of revisions to address new supply chain cyber security risks and mitigation measures, if any, related to industrial control system vendor products and services applicable to the Responsible Entity’s BES Cyber Cyber Systems; and

2.2. Obtaining CIP Senior Manager or delegate approval for any revisions to the plan(s).

Likes 0	

Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment
ERCOT supports the IRC comments on this question.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	

Comment
Generally, we agree with the requirement to have the CIP Senior Manager review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. However, R2.1 could be interpreted in many ways that might introduce uncertainty in the process. In agreement with EEI, we suggest the following language: R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	

Comment
Tacoma concurs with the comments provided by the LPPC.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, SMUD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

Seattle City Light agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, Seattle City Light requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities (CSU) agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CSU requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG agrees with the intent of this requirement, but has the following questions/recommendations below: • Recommend changing Requirement 2.1 from “Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and” to “Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures as determined by the registered entity; and”. • The standard language does not address how a revision to the plan needs to be addressed by contracts already in process/negotiation at the time of review or revision. Please provide guidance.	
Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

For consistency and to ensure that the requirement appropriately reflects the scope of risks being addressed, AZPS requests striking of ‘supply chain security risks’ in Requirement R2.1 and replacing with ‘Vendor security risks’.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

Santee Cooper agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, Santee Cooper requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Ballard Mutters - Orlando Utilities Commission - 3

Answer	Yes
Document Name	

Comment

OUC agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, OUC requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Devin Elverdi - Colorado Springs Utilities - 1

Answer	
Document Name	

Comment

Refer to CSU comments.

Likes 0	
Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1

Answer	
Document Name	

Comment

CPS Energy supports the comments provided by APPA

Likes 0	
Dislikes 0	
Response	

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Suggest “software, firmware, and associated patches” Possible TFE language for R3? The

NSRF recommends the following:

Q 3. Add language to address potential Technical Feasibility Exception (TFE).

R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware**, where technically feasible,** before being placed in operation on high and medium impact BES Cyber Systems:

R3.2

“Firmware” is already included in R3 this redundant in R3.2 recommend R3 to be written as a general Requirement with specifics in the sub Requirements.

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

The standard as written doesn’t clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	

TFE opportunity is again needed, especially to address vendor-proprietary (“black box”) vendor software and firmware, nor should there be any obligation to impose measures on vendors (see our “additional comments” responses).

R1.2.5 is largely duplicative of R3. They should be made consistent, or one of them should be deleted.

R3 may better belong in CIP-007 and needs to be aligned with CIP-010. Requirements for a single topic should be consolidated within a single standard.

Likes 0	
Dislikes 0	
Response	

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	

See APPA's, TAP's, and USI's comments.

Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John
Dislikes 0	
Response	

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	No
Document Name	
Comment	

It may not be possible to verify the integrity and authenticity of software and firmware before being placed into operation if the Vendor is no longer in business or will not cooperate. There should either be an exception or ‘*out’* for possibility (e.g. … where possible.), leaving that determination up to an audit team, or a feasibility exception should be allowed.

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

Change/add language to emphasize that failure to obtain the cyber security controls from a vendor doesn't translate to being out of compliance. Entity should have the ability to mitigate risks posed by vendors. Furthermore, this risk should be evaluated during the procurement and deployment of vendor products and services (CIP-013-1 R1), and mitigated as part of the CIP-007 R2.

IID feels that there should be an exclusion or exception (similar to a CIP Exceptional Circumstance or Technical Feasibility Exception) added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Would deployment tools that rely on digital signature enforcement (such as Microsoft Authenticode Security Verification or Red Hat signature verification) satisfy the intent of this requirement where such mechanisms provide technical checks for verification of authenticity and integrity?

The requirement measures should allow automated deployment tools such as Microsoft's System Center Configuration Management to be trusted for the purpose of confirming the integrity and authenticity of software and firmware.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy recommends the following language revision to R3.

"For BES Cyber Systems in production, each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware prior to installation on high and medium impact BES Cyber Systems:"

We suggest the addition of the phrase "For BES Cyber Systems in production," at the outset of the requirement.

We also recommend replacing the phrase "placed in operation" with "prior to installation" in R3. The phrase "placed in operation" is ambiguous, and could be open to debate as to what this actually means. The language "prior to installation" is less ambiguous, the language used in FERC Order 829, and is already used in the rationale section for this requirement.

Also, Duke Energy has some concern with the amount of involvement/cooperation that will be necessary from a vendor in order to achieve compliance with this requirement. Some issues may arise if/when a vendor is not able to verify the integrity or authenticity of a certain product. We suggest the drafting team consider this situation as appropriate for a Technical Feasibility Exception or in some instances be granted a CIP Exceptional Circumstance. For example, an issue could arise wherein an entity has a device that is failing, and a fix (update of software) is needed immediately. In the interest of system stability, there may not be enough time to wait on a vendor to send a certificate of authenticity on a patch or software upgrade. We feel that a Technical Feasibility Exception and CIP Exceptional Circumstance should be considered based on these issues.

Another aspect of R3 that we think requires some clarity is whether or not R3 should apply at the BES Cyber Asset level. Currently, the language explicitly states BES Cyber System, but we feel that the language may not represent the actual intent of the requirement. If the controls proposed in R3 are better suited at the Cyber Asset level, the language should be revised to reflect this.

Lastly, Duke Energy would like to suggest that the drafting team consider that this requirement be moved to current standard CIP-007-6. CIP-007-6 already addresses security controls for BES Cyber Systems, and we feel that this control oriented requirement may be better suited there.

Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

Requirement R3 mentions high and medium BES Cyber Systems, but does not include their associated Electronic Access Control and Monitoring Systems (EACMs), Physical Access Controls(PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following modifications for consideration:

1. R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems [and if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets]:

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

CIP-007 R2 requires a mitigation plan for patches that cannot be applied within 35 days. Please confirm that if a patch cannot be applied within 35 days due to the vendor's inability to provide the integrity check, there is no other compliance risk if the RE provides a mitigation plan in accordance with CIP-007 R2.

Additionally, if vendors refuse or can't provide hashes or other verification methods, please provide confirmation that an internal process to test, scan and perform verification activities would be enough to satisfy this requirement.

Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Response

ALAN ADAMSON - New York State Reliability Council - 10

Answer	No
Document Name	

Comment

See NPCC comments.

Likes 0	
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5

Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI urges the SDT to remove R3 and address firmware and software integrity/authenticity in the supply chain risk management plan(s) as detailed in the requirement concepts proposed by AECI in Question 1. This will allow Responsible Entities to address this issue contractually with applicable vendors in the supply chain/procurement process and not the operational time horizon.	
Likes 0	
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	

Answer	No
Document Name	
Comment	
PRPA requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Response	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	
AE requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No

Document Name	

Comment

1. R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2. How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business or will not cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date.

3. The applicability of this requirement should be limited to high and medium impact BES Cyber Systems with external routable connectivity. This would align the standard with the applicability of CIP-007 and CIP-010.

4. Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

5. Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

6. Provide clarity for when a system is pre-loaded by a vendor and delivered to an entity. Is the entity required to verify software authenticity? If a computer is purchased from Dell, can Dell provide authenticity for all of the firm ware that is part of the system but not directly manufactured by Dell; i.e. system bios, sound system, network adapter, video controller.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
This requirement should be incorporated into CIP-007 R2 or CIP-010 R1. This is a System Security Management requirement and belongs in the appropriate location. CIP-013-1 R3.1-R3.4 are all components of the the CIP-010 baseline. Placing this topic in a separate standard and requirement creates compliance confusion. As entities will have to follow different requirements in CIP-007, CIP-010, and CIP-013, there is an increased likelihood of a violation. As there is no consistency within the software industry on the use of hash functions, there must be guidelines on what is considered an acceptable approach to meet this requirement. While guidelines are needed, it must be understood that many times the individual utility has little influence on software vendors due to the relatively small purchasing power of the electric sector relative to the vendor's overall market.	
Likes 0	

Dislikes 0	
Response	
Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Response	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	

Comment

- The scope of CIP-013-1 R3 overlaps with parts of CIP-007-6 R2 and CIP-010-2 R1.1-1.5. However, both CIP-007 R2 and CIP-010 R1 apply to High and Medium BCS and associated EACMS, PACs, and PCAs. The potential collision of requirements that apply inconsistently (e.g. BCS vs EACMS) across three standards will be difficult to manage, monitor, and implement. For example, timing of security patch implementation per CIP-007 R2.3 could be impeded by authenticity processes required in CIP-013. Meeting compliance with CIP-013 could unintentionally cause not only potential compliance problems with CIP-007 R2, but also significant security, operational, and/or reliability impacts.
- An exception process is required for R3. This requirement will apply to the existing complement of High and Medium BCS, upon the enforcement date of the new Standard. However, since entities are explicitly not required to renegotiate existing contracts, it may be difficult to meet compliance with this requirement upon enforcement, if existing vendors do not provide appropriate support.
- Measures and Evidence – Since the R3 requires an entity to show that documented processes have been implemented, M1 does not adequately describe the evidence required to demonstrate implementation.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	

Comment

Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	

Comment
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	

Comment

1. R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.
2. How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations.

Does R3 allow the Entity to “accept the risk?”

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request “per system capability” wording for R3. Not all vendors provide a “golden hash” or other mechanism to validate.
- To be consistent with not requiring R1.2.5 we suggest adding the language “subject to procurement contract.”

To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.” There should be provisions to allow an entity to accept the risk of selecting a vendor that will not or cannot supply authentication.

Additionally, R3 may hinder an entity’s ability to meet the 35-day patch window in CIP-007-6 R2.2 and R2.3. In the case of a non-cooperative vendor, entities will be left in a position of choosing to violate CIP-013, R3 or CIP-007, R2.

Is R3 the implementation of R.1.2.5? Should there be more explicit tie-ins? Seems to be in conflict with provision in R1 where “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan”

We request clarification on relationships with resellers. Is verification of integrity and authenticity adequate from the reseller? Or does validation have to reach back to the original manufacturer?

Likes 0	
Dislikes 0	

Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Response	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx
Comment	
See comments n Requirement R3 in attached file.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST strongly supports the goal of verifying software integrity and authenticity and hopes vendors will be generally willing to provide Responsible Entities with checksums, cyber hash values, or other integrity checks for their software and firmware. However, as written the requirement creates the potential for a conflict with CIP-007-6 R2 Part 2.3 (installation of applicable security updates), and could leave a Responsible Entity with potentially no recourse other than to create a mitigation plan if a vendor is for some reason unable or unwilling to provide such integrity verification for a patch or other type of software or firmware update. N&ST recommends that the SDT consider allowing for exceptions that must be (a) fully documented and (b) approved by the Responsible Entity's CIP Senior Manager	
Likes 0	

Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	

Comment

We agree with the drafting team that verification to the integrity and authenticity of the software needs to be validated. However, we would ask the question, “If the industry finds validations issues, how do we hold the vendor accountable?” We understand that contracts are in place to help this situation, but this doesn’t always resolve validation issues. We feel that FERC Order 829 language falls short of holding the vendors accountable in reference to addressing verification of software integrity and authenticity and as a result, the compliance burden is placed on the users. The CIP requirements focus on the Responsible Entity carrying the compliance risk even if the industry can identify vendor validation issues. For example, entities could potentially pay for product upgrades to address compliance concerns when it’s been verified that the current product upgrades have not met the quality of service that was promised by the vendor. We suggest that the drafting team hold open discussions with FERC, potentially conducting a gap analysis in reference to this potential concern. If the analysis determines a gap, FERC should seek legislation to hold vendors more accountable.

Also, we suggest that Requirement R3 language should be moved to the CIP-010 Standard. Our group feels that the CIP-010 Standard adequately addresses software and firmware verification. Additionally, we propose some language revisions to the Requirement language.

SPP’s proposed language revision to R3:

“Each Responsible Entity shall implement one or more documented process for verifying the integrity and authenticity of the following software and firmware before being installed in operation on high and medium impact BES Cyber Systems”.

The term “installed” has been consistently used throughout the CIP-010 Standard and we feel this will give our proposed language validity and consistency.

Likes 0	
Dislikes 0	

Response

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch.

What does the SDT consider a "secure central software repository"?

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

The draft Requirement R3 language creates compliance concerns due to the need for Responsible Entities to negotiate commercial contracts with vendors that commit the vendors to undertake the tasks necessary for R3 compliance, particularly in circumstances where only a single vendor has the capability of providing the necessary services for Cyber Assets covered by CIP-013-1. For example, unless the vendor agrees to cooperate with any software integrity and authenticity verification process, the Responsible Entity will be unable to ensure the integrity and authenticity of software used in covered Cyber Assets.

Responsible Entities could encounter scenarios where:

• Vendors may refuse to comply with the Responsible Entity's vendor controls;

• Vendors may demand an unreasonably high payment for compliance with the Responsible Entity's vendor controls;

• Vendors may agree to Responsible Entity controls but fail to take the steps necessary to implement those controls in a compliant manner; or

- Software/firmware made by a vendor no longer in business and unable to assist the Responsible Entity in the integrity and authenticity verification process.

To ensure that compliance with CIP-013-1 does not place Responsible Entities in an untenable negotiating position, a compliance "safety valve" is necessary to allow Responsible Entities to comply with the Standard even in the absence of vendor assent to the Responsible Entity's required controls. Such a "safety valve" would be consistent with the current draft guidance on CIP-013-1 R1.2, which states that "[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Guidance language in the G&TB portion of a Standard is helpful, but the "safety valve" concept should be included within the language of the Requirement itself because only that language forms the basis of a compliance assessment.

Exelon has sent ideas under separate cover to the Drafting Team Chair outlining three options for providing the necessary "safety valve" along with proposed text edits to the requirements. In short, these options include a technical feasibility exception, a commercial feasibility exception or a simple exception documentation process.

Exelon does not support the draft language in R3 which requires an Entity to verify the integrity and authenticity before placing a BES Cyber System into operation. Instead, Exelon prefers the suggested language from Order No. 829 that directs "the integrity of the software and patches before they are installed in the BES Cyber System environment" (P. 48). Accordingly, Exelon suggests that R3 be edited to read as follows:

Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware **prior to installation into** high and medium impact BES Cyber Systems

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that for future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch.

What does the SDT consider a "secure central software repository"?

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

Specific operational cyber security controls are best addressed as revisions to CIP-002 through -011.

Prescribing verification of integrity and authenticity is a “how” not a “what.”

Refer to EEI comments on R3. We agree with the concept of the EEI comments to consider a revision in CIP-010 for a specific security objective (“what”), such as “method(s) to minimize the risk of installing compromised” CIP-010 R1 baseline configuration items.

We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives' deadlines, NERC and industry should reprioritize SDT teams' work and resources.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch.

What does the SDT consider a "secure central software repository"?

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

- Patch Management obligations for cyber security related patches are already addressed in CIP-007. Dominion is of the opinion that the obligations in this requirement would be better placed (once it's determined what the obligations should be) in CIP-010 or CIP-007.
- If R3 is kept in CIP-013 and not moved to an existing CIP Standard, we recommend the following:

R3: Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following, prior to authorized installation on high and medium impact BES Cyber Systems and associated EACMSs, PCAs, and PACs: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

SCE&G agrees with the concerns and questions raised by the Edison Electric Institute (EEI), including the following:

"Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls. For example, the language could allow a Responsible Entity to use a vendor's website for verifying both integrity and authenticity, which will not protect against a Watering Hole attack, where the vendor's website has been compromised and both the

software and the integrity check are likely to be compromised. However, we note that the majority of vendors use their websites for software downloads and include the hashes for integrity checks on those websites. Members have had difficulty in getting vendors to change their practices, which makes this requirement difficult if not impossible for Responsible Entities to comply with…Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third part, a vendor."

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG recommends that the R3 and R4 technical/operation control requirements should be located in the associated standard to avoid misalignments or jeopardizing timeframes outline in the other standards such as patch management. For Example: R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4.

NRG requests clarification from SDT regarding what could/should an entity do if there is no process to verify the authenticity of software? In those cases, can an entity document their defense in depth strategies as a compensating measure? NRG recommends that SDT communicate in Measures that verification of authenticity could include a way to present in our processes other methods that may not actually be verification.

NRG recommends that SDT list ways that a Registered Entity can authenticate a source in the Measures section. NRG also recommends that SDT list that a Registered Entity should have a means to use putty, Debian, or things that don't have as tight of controls, (i.e. provide a checksum, and/or set a policy that they don't use open source code and requests clarification of how a Registered Entity would demonstrate that they had verified an authoritative source (i.e. open source) to the extent of what their capability would allow). For example, NRG recommends that SDT list examples in Measures section to include use of a layered approach of security and functional testing: For example start with a notification process, authenticity check of source, and use hash / checksum, then perform testing (but how does testing demonstrate authenticity? Answer – virus scan, etc (functional vs. security testing: A/V scan, logging, access, control). Lastly perform a scan from a vulnerability assessment tool. How does this prove integrity and authenticity of the software? NRG requests clarification in the standard requirement of when this requirement would become effective. NRG recommends that the SDT allow the Registered Entities additional time for vendor re-negotiations relating to supply chain for the purposes of enabling validation of integrity and authenticity of software and firmware.

NRG suggests that the R3 language should move to CIP-010. NRG requests clarification of whether testing is a valid form of verification. Additionally, we suggest the Requirement language to read as follows "Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being installed in operation on high and medium impact BES Cyber Systems". Each requirement should have a provision that allows an entity to accept the risk of selection a vendor that will not or cannot supply a control.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

1. R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2. How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations

3. Request clarification (in the Standard) on how the SDT expects current and past contract negotiations to impact R3

Does R3 allow the Entity to “accept the risk?”

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request “per system capability” wording for R3. Not all vendors provide a “golden hash” or other mechanism to validate.
- To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.” There should be provisions to allow an entity to accept the risk of selecting a vendor that will not or cannot supply authentication.

4. Additionally, R3 may hinder an entity’s ability to meet the 35-day patch window in CIP-007-6 R2.2 and R2.3. In the case of a non-cooperative vendor, entities will be left in a position of choosing to violate CIP-013, R3 or CIP-007, R2.

5. Is R3 the implementation of R.1.2.5? Should there be more explicit tie-ins? Seems to be in conflict with provision in R1 where “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan”

6. We request clarification on relationships with resellers. Is verification of integrity and authenticity adequate from the reseller? Or does validation have to reach back to the original manufacturer?

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5

Answer	No
Document Name	

Comment

Same as RoLynda Shumpert's comments from SCE&G:

SCE&G agrees with the concerns and questions raised by the Edison Electric Institute (EEI), including the following:

"Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls. For example, the language could allow a Responsible Entity to use a vendor's website for verifying both integrity and authenticity, which will not protect against a Watering Hole attack, where the vendor's website has been compromised and both the software and the integrity check are likely to be compromised. However, we note that the majority of vendors use their websites for software downloads and include the hashes for integrity checks on those websites. Members have had difficulty in getting vendors to change their practices, which makes this requirement difficult if not impossible for Responsible Entities to comply with…Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third part, a vendor."

Likes 0	
Dislikes 0	

Response

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch.

What does the SDT consider a "secure central software repository"?

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	

Comment

1) R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2) How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations

3) Request clarification (in the Standard) on how the SDT expects current and past contract negotiations to impact R3

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

R3 applies whether revised contract terms and conditions exist or not, with no exception for vendor capability issues, technical feasibility, or situations where there is no vendor. It is also not clear whether changes that are not firmware or software versions or patches fall under the requirement. CenterPoint Energy requests that the phrase “where technically feasible” be added to Requirement 3.

Furthermore, the Company believes verifying software integrity and authenticity as described in CIP-013 R3 belong in CIP-010 and recommends aligning the R3 sub-requirements to match the items in CIP-010 R1.

It is not clear what an entity must do if the vendor will not or cannot assist by providing an authentication method. Having a verification requirement for R3.4, where not automatically supported by vendors, slows down the existing patch management process. This increases security risks by leaving systems unpatched against known vulnerabilities for longer periods and increases compliance risks for entities where dated mitigation plans must be used to document delays.

Additionally, it is not clear whether secure boot capability, default on many Cyber Asset operating systems, is adequate (or even required) to demonstrate compliance with software verification requirement.

CenterPoint Energy recommends that R3 be revised for flexibility and feasibility. It should also be moved to CIP-010 as these requirements would seem to fit as a part of existing configuration change management processes.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Ballard Mutters - Orlando Utilities Commission - 3

Answer	No
Document Name	

Comment

OUC requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

CIP-013-1 Requirement R3 is written with an assumption that the supplier provides a mechanism in which verification of integrity and authenticity can be performed on software and firmware. These tools/mechanism may not always be available to the Registered Entity, and the Registered Entity may not have the power in which to force the supplier to provide a verification method. Consistent with currently approved and enforceable CIP Cyber Security Reliability Standards, ATC recommends the SDT consider adding language to provision for conditions where it is not technically possible to perform a verification in order to provide the flexibility needed to preclude an impossibility of achieving compliance.

Additionally, the inclusion of "firmware" within the proposed language in CIP-013-1 R3 is an expansion in scope from the **first directive** in FERC Order No. 829 (P.2), which directed NERC to draft a new or modified Reliability Standard that "…should address the following security objectives, discussed in detail below: **(1) software integrity and authenticity;** (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

Additionally, CIP-013-1 Requirement R3 is simultaneously duplicative and additive with currently approved and enforceable CIP-010-2 Requirement R1 and the Applicable Systems within CIP-010-2 Requirement R1 Parts 1.1 – 1.5 as consequence of the broad reference to "high and medium impact BES Cyber Systems" without consideration of the construct of the CIP-010-2 Standard.

1. CIP-013-1 Requirement R3 Sub Requirements R3.1 – R3.4 are duplicative of CIP-010-2 Requirement R1 Parts 1.1 – 1.2, which obligates Registered Entities to develop and maintain a baseline of 'software' information for both high and medium impact BES Cyber Systems, where the types of software are effectively the same as what is being proposed.

    - CIP-010-2 Requirement R1 Part 1.5 addresses the testing of changes to this 'software' and 'firmware' for high impact BES Cyber Systems, rendering Sub Requirement R3.1 – R3.4 superfluous and unnecessary. Consequently, Requirement R3.1 – R3.4 also creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-010-2 Requirement R1 Part 1.5. In

its redundancy, it is at odds with the former efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

- CIP-010-2 Requirement R1 Part 1.5 has a provision to allow for the testing of this software and firmware in production where it is not technically feasible to perform testing in a test environment. CIP-013-1 R3 is effectively an expansion in scope to CIP-010-2 Requirement R1 Part 1.5 in its obligation to perform testing "…**before being placed in operation on a high** … …**impact BES Cyber System**". Any expansion in scope to access requirements or controls for high impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-010-2 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

- CIP-010-2 Requirement R1 Part 1.5 is not applicable to medium impact BES Cyber Systems. CIP-013-1 R3 is effectively an expansion in scope to CIP-010-2 Requirement R1 Part 1.5 in its obligation to perform testing "…**before being placed in operation on a… …medium impact BES Cyber System**". Any expansion in scope to access requirements or controls for medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-010-2 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

Likes 0	
Dislikes 0	

Response

Brian Bartos - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli

Answer	No
Document Name	

Comment

Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	

Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016.

Reclamation recommends Requirement R3 should instead require entities to review and update as necessary their supply chain risk management plan(s) developed in Requirement R1 at least once every 15 months.

Within each Requirement, the sub-requirements should distinguish between high, medium, and low impact BES Cyber Systems and other supporting systems. Reclamation recommends the implementation plan enforcement dates be staggered based on high, medium, and low impact for auditing purposes and to allow the associated risks and severity levels to be spelled out more clearly.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

Rationale for Requirement R3:

The rationale language for R3 states, “The objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.” R1, R2, and the Rationale for Requirement R3 do not specify the impact classification (High, Medium and Low) when referencing the BES Cyber System. R3 specifically states the impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems.” IPC would like know if the inconsistent impact classification references were intended or were an oversight by the SDT.

R3

The requirement language for R3 states, “before being placed in operation on high and medium impact BES Cyber Systems.” R1, R2, and the Rationale for Requirement R3 do not specify the impact classification (High, Medium and Low) when referencing the BES Cyber System. R3 specifically states the

impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems.” IPC would like know if the inconsistent impact classification references were intended or were an oversight by the SDT.

The requirement language for R3 states, “Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware." IPC is concerned that the SDT developed a standard that requires Responsible Entities to “verify the integrity and authenticity” of software and firmware of which Responsible Entities have no oversight or control over what each vendor provides.

IPC does not feel CIP-013-1 is an appropriate standard to address R3. IPC believes this requirement belongs in CIP-007-6 or CIP-010-2 as R3 is related to patching or configuration change management. IPC feels the intent of CIP-013-1 is to address supply chain controls, whereas CIP-007-6 and CIP-010-2 address testing and verification of changes controls, which are typically performed by technical staff as they test, implement, and update systems.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

LCRA supports ERCOT’s comments. CIP-013 R3 directly impacts baseline data and as such should be located within CIP-010.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
1) How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business or will not cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. 2) The applicability of this requirement should be limited to high and medium impact BES Cyber Systems with external routable connectivity. This would align the standard with the applicability and risk-based approach of CIP-007 and CIP-010. 3) Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011. 4) Provide clarity for when a system is pre-loaded by a vendor and delivered to an entity. Is the entity required to verify software authenticity? If a computer is purchased from Dell, can Dell provide authenticity for all of the firm ware that is part of the system but not directly manufactured by Dell; i.e. system bios, sound system, network adapter, video controller.	
Likes 0	
Dislikes 0	
Response	

Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	

Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No
Document Name	
Comment	

See EEI comments

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities

Answer	No
Document Name	

Comment

Colorado Springs Utilities (CSU) requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Within the Rationale, the word “ensure” is inappropriate. Even good controls do not “ensure” a desired outcome. It should also state that “software being installed in the BES Cyber System was not modified or altered without the knowledge of the supplier AND the recipient or licensee. Consider replacement of “ensure” with “confirm”.

R1. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. To address these concern, The IESO request that the SDT consider the use of provisional language to protect Responsible Entities such as use of a TFE.

R1. The SDT should consider the use of “validate” instead of “verify” in this requirement.

R1. The SDT should address situations that are outside the usual upgrade and patch processes. This includes the obligations for signature updates, and where a vendor brings code onsite (binary or source code) that the entity is not allowed to review.

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
Seattle City Light requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	

FMPA agrees with comments submitted by American Public Power Association.

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment

The NYPA Comments

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	
Comment	

Security Objective

Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls.

The authenticity verification is already addressed in the procurement and vendor risk assessment process. Based on the vendor provided information in 1.1.5, 1.2 should identify the method or source to obtain the software that provides reasonable assurance of the authenticity of the vendor provided software.

Methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in test environment prior to installation on applicable assets, etc.

We recommend the following language for consideration by the SDT:

R3. Prior to installing new (1) operating systems(s); (2) firmware; (3) commercially available or open-source application software; and (4) patches, updates and upgrades to these, use one or more documented method(s) to minimize the risk of adversely or unintentionally modified software.

Requirement Placement (CIP-010)

Requirement R3 may also fit better within CIP-010 (e.g., after R3, Part 3.3) since it is more of an operational security control. However, the security objective for this requirement is focused on risk the vendor may introduce by delivering software that has been altered before or during transit to the Responsible Entity so keeping it in a separate, supply chain standard may also make sense. Also, to implement R3, Responsible Entities will likely need to work with the vendor during procurement (R1 and R2) to ensure that they can meet R3.

Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third party, a vendor.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	
Comment	

Tacoma concurs with the comments provided by the LPPC.

Likes 0	
Dislikes 0	

Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language. Furthermore, operational checks to verify security controls are not adversely affected are covered in other CIP standards.	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA supports ERCOT's comments. CIP-013 R3 directly impacts baseline data and as such should be located within CIP-010.	
Likes 0	
Dislikes 0	
Response	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	
Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls.	

The authenticity verification is already addressed in the procurement and vendor risk assessment process. Based on the vendor provided information in 1.1.5, 1.2 should identify the method or source to obtain the software that provides reasonable assurance of the authenticity of the vendor provided software.

Methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in test environment prior to installation on applicable assets, etc.

We recommend the following language for consideration by the SDT:

R3. Prior to installing new (1) operating systems(s); (2) firmware; (3) commercially available or open-source application software; and (4) patches, updates and upgrades to these, use one or more documented method(s) to minimize the risk of adversely or unintentionally modified software.

Requirement Placement (CIP-010)

Requirement R3 may also fit better within CIP-010 (e.g., after R3, Part 3.3) since it is more of an operational security control. However, the security objective for this requirement is focused on risk the vendor may introduce by delivering software that has been altered before or during transit to the Responsible Entity so keeping it in a separate, supply chain standard may also make sense. Also, to implement R3, Responsible Entities will likely need to work with the vendor during procurement (R1 and R2) to ensure that they can meet R3.

Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third party, a vendor.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No
Document Name	

Comment

Within the Rationale, the word "ensure" is inappropriate. Even good controls do not "ensure" a desired outcome. It should also state that "software being installed in the BES Cyber System was not modified or altered without the knowledge of the supplier AND the recipient or licensee. Consider replacement of "ensure" with "confirm".

R1. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. To address these concern, The IRC and SWG request that the SDT consider the use of provisional language to protect Responsible Entities such as use of a TFE.

R1. The SDT should consider the use of “validate” instead of “verify” in this requirement.

R1. The SDT should address situations that are outside the usual upgrade and patch processes. This includes the obligations for signature updates, and where a vendor brings code onsite (binary or source code) that the entity is not allowed to review.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls.

The authenticity verification is already addressed in the procurement and vendor risk assessment process. Based on the vendor provided information in 1.1.5, 1.2 should identify the method or source to obtain the software that provides reasonable assurance of the authenticity of the vendor provided software.

Methods to minimize the integrity risk is determined based on the vendor and Responsible Entity’s capability and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in test environment prior to installation on applicable assets, etc.

We recommend the following language for consideration by the SDT:

R3. Prior to installing new (1) operating systems(s); (2) firmware; (3) commercially available or open-source application software; and (4) patches, updates and upgrades to these, use one or more documented method(s) to minimize the risk of adversely or unintentionally modified software.

Requirement Placement (CIP-010)

Requirement R3 may also fit better within CIP-010 (e.g., after R3, Part 3.3) since it is more of an operational security control. However, the security objective for this requirement is focused on risk the vendor may introduce by delivering software that has been altered before or during transit to the Responsible Entity so keeping it in a separate, supply chain standard may also make sense. Also, to implement R3, Responsible Entities will likely need to work with the vendor during procurement (R1 and R2) to ensure that they can meet R3.

Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third party, a vendor.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC disagrees with the proposed requirement. CIP-013-1 R3 requires actions to be taken by the Responsible Entity that are outside of the supply chain context. Paragraph 45 of Order No. 829, specifies this objective of software integrity and authenticity should be applied to “The Plan” identified in the core directive in the context of addressing supply chain management risks. The SDT has chosen to identify controls in R3 that are executed only as part of the day-to-day management of BES Cyber Systems. These controls fail to effectively address the security objective of addressing software integrity and authenticity, will have minimal security value, are administratively burdensome on industry, and are inconsistent with the supply chain context. SAFECode’s (http://www.safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf) Software Integrity Control’s whitepaper outlines controls that effectively address software integrity and authenticity. Nearly all of these controls must be implemented by the vendor. As such, Responsible Entity’s should have the flexibility to require the vendor to provide software assurance through contractual means. Such as “supplier provides customer ways to differentiate genuine from counterfeit software”

Unfortunately, the SDT has not provided controls that effectively address software integrity and authenticity and has instead focused its control as demonstrated by the language in the measure on ensuring the “entity performed the actions.” In order to provide entities the flexibility to effectively address the security risks associated with the supply chain, we respectfully request that the SDT revise its draft standard to be more in line with the framework identified in FERC Order 829. Our recommendation, consistent with our response to question 1, is as follows

GTC recommends the SDT reconsider relocating the attributes of R3 in a manner that addresses the security objective to “The Plan” specified in R1 to align with the FERC Order. This would allow the Responsible Entity to handle contractually with the vendor i.e. “supplier provides customer ways to differentiate genuine from counterfeit software (such as digital signatures)”. Our recommendation is consistent with our response to question 1, which is summarized as follows:

See GTC’s comment for Question #1.

Upon close review of FERC's directives summarized beginning on paragraph 43 through paragraph 62, the Order essentially directs this new Standard as outlined:

Paragraphs 43 – 45:

R1: Develop a plan to include security controls for supply chain management that address controls for mitigating Supply Chain risks to hardware, software, and computing and networking services which are intended to support Bulk Electric System operations; that include the following four specific security objectives in the context of addressing supply chain management risks:

R1.1 Security objective 3 (*information system planning*)

R1.2 Security objective 4 (*vendor risk management and procurement controls*)

R1.3 Security objective 1 (*software integrity and authenticity*)

R1.4 Security objective 2 (*vendor remote access*)

Paragraph 43:

R2: Implement the plan specified in R1 in a forward looking manner.

Paragraphs 46 - 47:

R3: Review and update, as necessary its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months

R3.1 Evaluation of revisions…

R3.2 Obtaining CIP Senior Manager or delegate approval.

Paragraphs 48 – 50:

FERC prescribes the various ways to address the first objective to the plan.

Paragraphs 51 – 55:

FERC prescribes the various ways to address the second objective to the plan.

Paragraphs 56 – 58:

FERC prescribes the various ways to address the third objective to the plan.

Paragraphs 59 – 62:

FERC prescribes the various ways to address the fourth objective to the plan.

FERC goes on to respond to comments on Existing CIP Reliability Standards, beginning with paragraph 71, “while we recognize that existing CIP Reliability Standards include requirements that address aspects of supply chain management, we determine that existing Reliability Standards do not adequately protect against supply chain risks that are within a responsible entity’s control. Specifically, we find that existing CIP Reliability Standards do not provide adequate protection for the four aspects of supply chain risk management that underlie the four objectives for a new or modified Reliability Standard discussed above.” FERC summary continues to focus on CIP-013-1 being limited to aspects of supply chain risk management.

Likes 0	
Dislikes 0	

Response

Bob Case - Black Hills Corporation - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The NERC Entity is the customer of the hardware supplier and software supplier, not the designer, manufacturer and developer of what is being procured. As such, the Entity can only clearly state what they want the hardware and software to do – at a high level, likely derived from what the vendor said there product could do, along with the expectation that the product will be “bug free”. But the Entity should not be expected to have the expertise and tools to “verify the integrity and authenticity of software and firmware”. Integrity and authenticity can only be assured by each link backwards in the Supply Chain, and collectively that will only happen if each link of the Supply Chain agrees to control their link. CIP-013 is not in a position to impose those controls on the entire Supply Chain, but only on the end customer - NERC Registered Entity. That said, software and firmware should be expected to be checked for proper "functionality" by the Registered Entity, per past CIP practice.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich

Answer	No
Document Name	

Comment

See comments submitted by Black Hills Corporation

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	
Comment	

This Standard, and therefore this Requirement needs to be squarely focused on the vendor product or service being procured and not on the categorization of a BES Cyber System. Requirement R3 should not be limited to High and Medium Impact BES Cyber Systems. A SEL-421 is a SEL-421 and the same risks of procurement, including firmware updates, apply to all SEL-421s impacted regardless of where they are deployed. Software/firmware updates are often acquired once and widely deployed. This is especially true in the substation environment where the exact same firmware release will be used to update Medium and Low Impact relays.

Likes 0	
Dislikes 0	
Response	

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick

Answer	No
Document Name	
Comment	

Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra

Answer	No
Document Name	
Comment	

1) R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2) How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations

3) Request clarification (in the Standard) on how the SDT expects current and past contract negotiations to impact R3

Does R3 allow the Entity to “accept the risk?”

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

· Request “per system capability” wording for R3. Not all vendors provide a “golden hash” or other mechanism to validate.

· To be consistent with not requiring R1.2.5 we suggest adding the language “subject to procurement contract.”

To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.” There should be provisions to allow an entity to accept the risk of selecting a vendor that will not or cannot supply authentication.

Additionally, R3 may hinder an entity’s ability to meet the 35-day patch window in CIP-007-6 R2.2 and R2.3. In the case of a non-cooperative vendor, entities will be left in a position of choosing to violate CIP-013, R3 or CIP-007, R2.

Is R3 the implementation of R.1.2.5? Should there be more explicit tie-ins? Seems to be in conflict with provision in R1 where “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan”

We request clarification on relationships with resellers. Is verification of integrity and authenticity adequate from the reseller? Or does validation have to reach back to the original manufacturer?

Likes 0	
Dislikes 0	

Response

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6

Answer	No
Document Name	

Comment

For a smaller CIP applicable medium impact BES Cyber System, we apply between 5,000 and 7,000 patches a year. The only feasible means for us to apply any meaningful integrity check is through automated, cryptographic mechanisms. This is a good practice, which should be followed, but we haven't found a good adoption rate by the Vendors developing the software. Even still, authenticity controls do very little without better software development lifecycle controls in place by the vendor. Additionally, the poor record of Certificate Authorities to control certificate validation should be raised.

The cost of putting a process like this in place involves a heavily centralized procurement team and the time to research a large number of vendor practices pertaining to verification. We do not believe the risk reduction justifies this very costly requirement. We propose meeting the FERC directive through R1 and dropping this Requirement altogether.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5

Answer	No
Document Name	

Comment

See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

The NERC Entity is the customer of the hardware supplier and software supplier, not the designer, manufacturer and developer. As such the Entity can only clearly state what they want the hardware and software to do – at a high level, likely derived from what the vendor said it could do, plus expecting that it will be "bug free". But the Entity should not be expected to have the expertise and tools to "verify the integrity and authenticity of software and firmware" – that is required to be ensured by each step back in the Supply Chain, and that will only happen if each link of the Supply Chain agrees to control their link. CIP-013 is not in a position to impose those controls on the Supply Chain, but only on the end customer. Software and firmware should be expected to be checked for functionality by the Entity.

Likes 0	
Dislikes 0	

Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	

Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes this Requirement is already covered in CIP-007. Having a CIP-013 requirement, that if violated, opens the door to double jeopardy (a finding in CIP-013 would also lead to a finding in CIP-007). There is no need for this Requirement. If there are additional requirements that must be identified, then CIP-013 is not the place for it, CIP-007 is a more appropriate place.	
Likes 0	
Dislikes 0	

Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 3. In addition, we offer the following comments: **Ambiguous Language – "integrity" and "authenticity"**	

The crux of the Requirement is to develop and implement plan(s) that address verification of the “integrity” and “authenticity” of operating systems, firmware, open-source software, and certain patches and upgrades prior to use. Without defining or providing a framework as to what “integrity” and “authenticity” mean, the terms are not measurable for CMEP purposes.

We suggest the Requirement include language that points to established and accepted security frameworks and standards. We offer the following alternative language:

R3. Each Responsible Entity shall manage its Cyber Asset Systems supply chain informed by well-established and accepted cyber security frameworks and standards for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems:

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Concur with EEI’s Position

Likes 0	
Dislikes 0	

Response

Val Ridad - Silicon Valley Power - 1 - WECC

Answer	No
Document Name	

Comment

see APPA's comments, with which SVP agrees.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

R3 – line 2 – for clarity purposes NRECA recommends removing “software and firmware.”

Additionally, to the extent possible, NRECA recommends that this requirement should be incorporated into CIP-007 R2 or CIP-010 R1. This is a System Security Management requirement and belongs in the appropriate location. CIP-013-1 and R3.1-R3.4 are all components of the CIP-010 baseline. Placing this topic in a separate standard and requirement creates compliance confusion.

Likes 0	
Dislikes 0	

Response

Luis Rodriguez - El Paso Electric Company - 6

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

In addition, the concerns expressed by EPE in response to Requirement 1 with respect to the proposed verification requirements also applies with respect to Requirement 3. Requiring a Responsible Entity to have a process to address verification is different from making a Responsible Entity responsible for software and firmware verification. EPE has had experiences in the past where the developers/vendors of software products provided to EPE products that they considered authentic and to have integrity. EPE’s testing in a strong test environment (before the products were placed in service) did not reveal any errors, yet, as the products were placed in service, errors were revealed that could not be explained *by the software developers themselves*. Under the new standard, as worded currently, would this experience create an instance of noncompliance? If so, how would a Responsible Entity avoid being noncompliant in a situation in which the product vendor created the product and still could not predict or explain the error?

As EEI explains in its comments, methods to minimize the integrity risk is determined based on the vendor and Responsible Entity’s capability, and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in a test environment prior to installation on applicable assets, etc. If a Responsible Entity may satisfy its compliance responsibilities for integrity verification through such methods, the requirement should be recrafted with language that makes this clear to the Responsible Entity.

Likes 0	

Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

In addition, the concerns expressed by EPE in response to Requirement 1 with respect to the proposed verification requirements also applies with respect to Requirement 3. Requiring a Responsible Entity to have a process to address verification is different from making a Responsible Entity responsible for software and firmware verification. EPE has had experiences in the past where the developers/vendors of software products provided to EPE products that they considered authentic and to have integrity. EPE's testing in a strong test environment (before the products were placed in service) did not reveal any errors, yet, as the products were placed in service, errors were revealed that could not be explained *by the software developers themselves*. Under the new standard, as worded currently, would this experience create an instance of noncompliance? If so, how would a Responsible Entity avoid being noncompliant in a situation in which the product vendor created the product and still could not predict or explain the error?

As EEI explains in its comments, methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability, and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in a test environment prior to installation on applicable assets, etc. If a Responsible Entity may satisfy its compliance responsibilities for integrity verification through such methods, the requirement should be recrafted with language that makes this clear to the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant

Answer	No
Document Name	

Comment

We don't believe it is reasonable to expect entities to be able to "verify" the integrity and authenticity of software and firmware in all cases. We can attempt to minimize the risk and/or provide reasonable assurance that we have received what was intended. There also needs to be a recognition of the many varied ways that updates and installations of software and firmware might be done most effectively, including the use of automated solutions.

Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

In addition, the concerns expressed by EPE in response to Requirement 1 with respect to the proposed verification requirements also applies with respect to Requirement 3. Requiring a Responsible Entity to have a process to address verification is different from making a Responsible Entity responsible for software and firmware verification. EPE has had experiences in the past where the developers/vendors of software products provided to EPE products that they considered authentic and to have integrity. EPE's testing in a strong test environment (before the products were placed in service) did not reveal any errors, yet, as the products were placed in service, errors were revealed that could not be explained *by the software developers themselves*. Under the new standard, as worded currently, would this experience create an instance of noncompliance? If so, how would a Responsible Entity avoid being noncompliant in a situation in which the product vendor created the product and still could not predict or explain the error?

As EEI explains in its comments, methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability, and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in a test environment prior to installation on applicable assets, etc. If a Responsible Entity may satisfy its compliance responsibilities for integrity verification through such methods, the requirement should be recrafted with language that makes this clear to the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT supports the IRC comments on this question and offers the following supplemental comments.

ERCOT recognizes the need for the concepts contained in Requirement R3. However, ERCOT disagrees with the placement of the requirement in a new standard. Since this requirement is applicable to only high and medium impact BES Cyber Systems, it should be placed within CIP-010. The requirement directly impacts the baselines that have been established within CIP-010 R1. The SDT could insert a new part between existing Parts 1.1 and 1.2 in that standard. The new part could use the following language: “For any updates or patches that that deviate from the existing baseline configuration, verify the authenticity and integrity of the update or patch.” As mentioned previously, in developing the CIP Version 5 standards, the SDT performed extensive work to ensure that all requirements related to a particular subject were included in one standard instead of being spread across multiple standards. The proposed language will disrupt that framework. Including the requirement in CIP-010 will ensure that a single standard captures all parts of the change process, including inventory (Part 1.1), validation of the code (NEW), authorization of implementation (Part 1.2), update of the inventory (Part 1.3), and testing of the change (Parts 1.4 and 1.5). This approach would give Responsible Entities a complete view of what is required from the start to the end of a change. It also prevents entities from keeping separate inventories to meet the CIP-010 requirement and the CIP-013 requirement.

Additionally, ERCOT requests guidance on how to demonstrate compliance when using automated solutions to obtain the most current patches applicable to their systems. In large environments, these automated solutions are critical to meeting the timing obligations of CIP-007 R2. Inserting the manual step of verifying integrity and authenticity of updates and patches can prevent the use of these solutions that entities have invested in and rely upon for addressing security risks and regulatory obligations. If it is intended that the entity may simply document the source used by these solutions, it would be helpful to put such clarifying language in the requirement.

Additional use cases for the SDT to consider in developing guidance include: (1) how signature and pattern updates are contemplated within the requirement since these are not updates to the operating system, software, or firmware noted, (2) instances when code is packaged and mailed to an entity, (3) software and firmware that are part of a vendor black-box type of appliance solution where the entity has no visibility to the code on the device, and (4) vendors bringing code onsite that the entity is not allowed to review. Any of these cases could present an obstacle to strict compliance with the draft standard language.

As with Requirement R1, this requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. The drafting team should address situations in which vendors will not or cannot provided the levels of service mandated by this requirement. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R3. NERC’s Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company disagrees with the direction the proposed R3 requirement is taking. Given our previous comments under R1 regarding the proper scoping of this new Standard to the “Supply Chain” time horizon, actions proposed to be required under R3 fall outside of that time horizon where the controls are applicable to BES Cyber Systems, which are not yet designated or commissioned as such. Additionally, R3 requires the development of “one or more documented processes” that are in addition to “the plan(s)” required in R1; Southern recommends maintaining the proper scoping of this Standard by moving the components of R3 under R1 to be addressed by the Responsible Entity in “the plan(s).”

If R3 is not consolidated under the R1 requirements for “the plan(s)” to be applicable within the Supply Chain time horizon, then Southern provides the following recommended edits to maintain vital consistency with existing requirements under CIP-010 R1.1. There is firmware in every video card, mouse, hard drive, etc. that is NOT the objective of the requirements in this Standard, but could, without the qualification provided below, be included. The addition under R3.2 also provides vital consistency with CIP-010 R1.1 so we aren’t maintaining different baseline configurations on all of our systems because of slightly different wording in the two Standards.

In this situation where very similar requirements in two different standards create additional administrative burden on entities, the SDT needs to recognize and address the delays that the proposed R3 requirements will have on the existing requirements under CIP-007-6 R2 (Patch Management). The burden of verification of integrity and authenticity of software and firmware in front of applicable requirements for determining availability, applicability, and conducting deployment of security patches within 35 day cycles will make those existing requirements under CIP-007-6 R2 unmanageable and will increase the administrative burden of creating patch mitigation plans as a result of competing Standards.

Modify R3 language as follows:

R3. Each Responsible Entity shall implement one or more documented process(es) that addresses the verification of the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

3.1 Operating System(s) or firmware where no independent operating system exists;

3.2 Commercially available or open-source application software intentionally installed; and

3.3 Patches, updates, and upgrades to 3.1 and 3.2.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 5

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment
We agree with this in principal, but this requirement will be extremely difficult to implement and ensure compliance. Currently, numerous vendors do not provide digitally signed patches (Microsoft is notorious for this) or other hashes to verify that a file was not modified. The ability to verify 100% of all software and files will be impossible until vendors are required to implement digital signatures. This can be done via contracts, but it will take time. We highly recommend that the requirement be changed to allow for the fact that software may not be able to be verified and that as long as an entities process checks for this that it is still valid to install with risks.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	

Comment
This appears to be a reasonable approach to meeting the FERC directive.

Likes 0	
Dislikes 0	

Response

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
No Comments

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	

Comment
What other measures or documented evidence should be expected by the Regional Entities when evaluating R3 at audit? An entity could leverage existing CIP-010-2 R1 (3.1-3.3) baseline controls and CIP-007-6 R2 patch management (3.4) controls to support the integrity and authenticity of software and firmware as specified in the CIP-013-1 R3 requirement. However, since the baseline configurations are developed and managed at the BCS level, it is possible that a change to the baseline configuration(s) of a vendor supplied system may not trigger a change to the corresponding baseline configuration for the BCS to which the system(s) is assigned. Therefore, relying on changes to the baseline configuration(s) may not (by itself) be a reliable control to determine if changes were made to a new vendor-supplied system. In such cases, the addition of a simple control (an extra check for new vendor-supplied systems) integrated into an entity's existing CIP-010-2 program would suffice to address the issue.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	

Comment
1. We favor industry accepted methods to address software authenticity such as digital signatures that are consistent with other critical sectors.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment
BPA proposes that to truly isolate the production systems from compromised software or firmware more prescriptive language than ‘before being placed in operation’ is required. BPA recommends the SDT develop language to address a supplier that is unwilling or able to support the requirement.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	

Comment

AZPS notes that Requirement R3 requires documented processes for verifying the "integrity and authenticity" of software and firmware before being place into operation and that such language may result in redundant verifications and processes. In particular, software, firmware, etc. are often verified when they are received from the vendor and "incubated" on low risk systems before being pushed to BES Cyber Systems. To avoid the need to "re-verify" these updates after incubation, but prior to placement in production on BES Cyber Systems, AZPS requests the following change to Requirement R3,

'…verifying the integrity and authenticity of the following software and firmware ***being placed in operation on high and medium impact BES Cyber Systems***, **when received**'. Additionally, Requirement R3 addresses the verification of integrity and authenticity of software and firmware; however, it does not address the likelihood of a vendor's inability or unwillingness to comply. AZPS requests clarification of whether an inability to verify would be considered a failure to implement the process if verification is not possible due to vendor inability or unwillingness.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

PSEG agrees with the intent of this requirement, but has the following questions/recommendations below:

- The way this requirement is written, it may not be possible to perform a technical verification of software integrity and authenticity. How does the standard drafting team expect registered entities to address this if it cannot be done in a technical manner?
- Requirements R1 and R2 do not require the registered entity to go back and revise previous contracts. In order to comply with this requirement, R3, changes to past contracts / vendor service agreements may be required. Alignment is needed between R1, R2, and R3.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	Yes
Document Name	

Comment

We recommend the SDT address virtualization and CIP Exceptional Circumstance with respect to this requirement aligned with project 2016-02.

Also please see our earlier comments with regards to redundancy between R3 and R1.2.5.

Likes 0	
Dislikes 0	

Response

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 5

Answer	
Document Name	

Comment

Suggest striking the word “associated” from the phrase “software, firmware, and associated patches”.

Basin Electric recommends adding language to address potential Technical Feasibility Exception (TFE) such as:

R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware**, where technically feasible,** before being placed in operation on high and medium impact BES Cyber Systems:

In R3.2, “Firmware” is already included in R3 which is redundant in R3.2. Basin Electric recommends R3 be written as a general Requirement with specifics in the sub Requirements.

There are a lot of parallels between these requirements and the requirements already required in CIP-007 R2 patch management controls. Basin Electric would rather see these obligations integrated into CIP-007.

The rationale explains the obligation for this requirement starts in the operate/maintain phase of the life cycle, but the timing/life cycle language is not included in requirement. Basin Electric suggests modifying the requirement to include clarification of when the obligation starts. Perhaps add language to the front of R3 such as: “For Cyber Assets in production…”

Likes 0	
Dislikes 0	

Response

Devin Elverdi - Colorado Springs Utilities - 1

Answer	
Document Name	

Comment

Refer to CSU comments.

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	
Response	

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

As written, R4 is more appropriately addressed in other existing standards, CIP-004 for authorization, CIP-005 for remote access, CIP-007 for logging, and CIP-008 for response. Furthermore, it confuses the expectation of all these standards from an audit perspective by duplicating or undermining existing requirements. Authorization for interactive remote access is already covered in CIP-004 R4. Logging and monitoring of access to an Intermediate System or BES Cyber Asset is already covered in CIP-007 R4. If an entity requires separate evidence for those standards and CIP-013 R4, this could present a double jeopardy situation for compliance where an entity can be audited and penalized twice for similar requirements if a Regional Entity does not find their methods of compliance satisfactory.

Controlling remote access, including vendor remote access, is already addressed in CIP-005 R1 and R2 so CIP-013 R4 will overlap with those existing requirements. CenterPoint Energy recommends changing “system-to-system remote access with a vendor” to “vendor initiated system-to-system remote access” and modifying existing requirements if necessary, rather than including the requirements in CIP-013.

R4.3 is part of an entity’s incident response plan, and should be in CIP-008.

R4.2, R4.3 sub-requirements both need clauses for per Cyber Asset capability or technical feasibility exceptions.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	
Comment	

1) R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.

2) Recommend that this Rationale needs to be updated from “machine-to-machine” to “system-to-system” for consistency

3) The first sentence of R2 is broader than the second sentence. The first sentence is “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems.” The second sentence is “The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):“ Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.

4) Request guidance. “Vendor-Initiated” could be considered a single word and not associated with the proposed definition of “vendor”.

5) Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to *detected* unauthorized activity.“

6) The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.

Likes 0	
Dislikes 0	
Response	

Richard Vine - California ISO - 2

Answer	No
Document Name	
Comment	

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	

Dislikes 0	

Response

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining “unauthorized activity” if that is not changed to “unauthorized access”.

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we must monitor every move,

such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5

Answer	No
Document Name	

Comment

Same as RoLynda Shumpert's comments from SCE&G:

SCE&G agrees with EEI in its assessment regarding R4:

"The use of "activity" in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as "escorted cyber access." In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions… We recommend that the SDT consider changing "activity" to "access" in parts 4.2 and 4.3."

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

1. R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.
2. Recommend that this Rationale needs to be updated from "machine-to-machine" to "system-to-system" for consistency
3. The first sentence of R2 is broader than the second sentence. The first sentence is "Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems." The second sentence is "The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):" Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.
4. Request guidance. "Vendor-Initiated" could be considered a single word and not associated with the proposed definition of "vendor".

5. Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to *detected* unauthorized activity.“

6. The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.

7. Consider eliminating sub requirements 4.1 and 4.2 since they are covered in CIP-005 and CIP-007, R5 respectively. Consider addressing sub requirement 4.3 by modifying CIP-005 thus eliminating R4 from the proposed CIP-013 standard.

8. R4 should be moved to CIP-005 since this requirement, as written in CIP-013, only applies to vendors having remote access. This does not address other sources of remote access threats as written.

9. For R4.2, we suggest limiting the retention period for evidence logs to 90 days to be consistent with CIP-007 R4, Parts 4.1, 4.2, and 4.3.

10. This would increase the scope of file integrity monitoring to Medium impact devices, some which are not capable of logging. This would discourage entities from allowing vendors to ever log in remotely, which might hinder reliability in the case of required emergency troubleshooting/support. Lack of timely support would also force entities to be non-compliant with other standards, such as other CIPs.

11. Remove vendor remote access from scope and only include system-to-system. Vendor remote access is already addressed in CIP-005 R2.

12. SDT appears to be building on top of CIP-005 R1.5; however, R4.3 says “during the remote access session,” which may not reasonable amount of time since this is a real-time action.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG suggests that R4, Section 4.1, Section 4.2, Section 4.3 language be moved to CIP-005. Since this is interactive remote session specific, NRG recommends moving all of these requirements into CIP-005 because of the implied real-time monitoring and logging requirements. Even though there are monitoring requirements in CIP-007, the monitoring requirements of CIP-007 are more forensic in nature. Various vendors and entities will likely want to implement individualized solutions to manage this requirement which will become administratively burdensome to the industry. These varied solutions can also present more ports being open (a reliability /security risk) to High and Medium BES Cyber Systems which could lessen reliability. NRG recommends that scope of this requirement should be for High and Medium with ERC BCS.

NRG requests that the SDT provide clarity that “system-to-system” is equivalent to “machine-machine” and what does it mean (i.e. application interface vs. laptop/server level). NRG recommends reference to the OSI layers. The R4 rationale appears to be inconsistent with the FERC directive regarding “machine to machine”. NRG requests clarification of whether the rationale / intent of “system-to-system” is meaning that a direct machine to machine interface is needed or that it needs to go through an intermediate or third host (jump host). NRG requests that the term “vendor” be defined to clarify intent of meaning a company or an individual (in the context of interactive remote access).

In the implementation plan for this standard, NRG recommends a staggered implementation plan for R1, R2 & , R5 being 15 calendar months. However, NRG recommends a 24-month implementation plan for R3 & R4would be needed for Registered Entities to manage this process on all impacted systems due to the need to re-negotiate processes with vendors (individualized solutions).	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
SCE&G agrees with EEI in its assessment regarding R4: *"The use of "activity" in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as "escorted cyber access." In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions… We recommend that the SDT consider changing "activity" to "access" in parts 4.2 and 4.3."*	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	
• Interactive Remote Access controls are defined in CIP-005 and in CIP-007. These requirements are duplicative and create the possibility of double-jeopardy for non-compliance. In addition, CIP-004-6 R4 Part 4.1.1 specifically addresses electronic access. Dominion is of the opinion that CIP-013-1 should concentrate on supply chain obligations for system-to-system communications which isn't addressed under the existing CIP standards. Operational requirements, such as the proposed R3, should be added to the appropriate CIP standard. • Dominion recommends removal of Part 4.2. Complying with the logging requirement could degrade system performance to the point where the BES reliability would be negatively impacted. Additionally, the monitoring requirement further degrades the performance, and may not be technically feasible. • If Part 4.2 is retained, the requirements should state the minimum criteria for logging and monitoring unauthorized access, as currently outlined in CIP-007-6 Part 4.1.	

- The terms “access” and “activity” as used in the proposed CIP-013-1 need to be defined.
- Read only access should be excluded from the final requirement based on definition of Interactive Remote Access.
- Dominion recommends the removal of Part 4.3 Disabling or otherwise responding to unauthorized activity during remote access sessions seems to imply an on-going monitoring of active connections to a degree that’s not technically feasible.
- If Part 4.3 is retained, we recommend that the minimum criteria for logging and monitoring be limited to disabling what has been detected. Dominion recommend the following language to achieve this goal:

4.3: Disabling or otherwise responding to detected, logged, and monitored unauthorized activity during remote access sessions.

- Dominion recommends creating a definition “system-to-system remote access” in the NERC glossary. Using a broad undefined term can lead to inconsistent results.

Likes 0	
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining “unauthorized activity” if that is not changed to “unauthorized access”.

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we must monitor every move, such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

Specific operational cyber security controls are best addressed as revisions to CIP-002 through -011.

Refer to EEI comments on R4 which point out overlaps to existing requirements in CIP-004, -005 and -008.

We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives’ deadlines, NERC and industry should reprioritize SDT teams’ work and resources.

We further point out the FERC Order 829 has directed revisions to remote access (for vendors) by Sept. 2017 which is before FERC’s Order 822 P64 directive to NERC for a CIP version 5 remote access controls effectiveness study is even due. The remote access controls effectiveness study is not due till June 30, 2017.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining “unauthorized activity” if that is not changed to “unauthorized access”.

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we must monitor every move,

such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

The proposed Requirement creates significant overlap with existing CIP Requirements. Requirement R4, as well as Requirements R3 and R5, should be modified so that CIP-013 only addresses those aspects of software integrity and authenticity (R3), remote access (R4), and authenticity and remote access for low impact BES Cyber Systems (R5) not covered by other Standards. Exelon understands that the timeframe dictated by FERC in Order No. 829 does not allow for revisions by this SDT to the relevant Standards that address these topics. However, overlap between the Standards should be avoided as much as possible to avoid double jeopardy concerns in the event of potential non-compliance with CIP-013 R3, R4, and R5.

For example, Exelon's review of the draft CIP-013-1 Standard indicates the following areas of overlap:

• CIP-013-1 R3.1 through R3.4 require authentication of operating systems, firmware, software, and patches. However, the configuration change management requirements under CIP-010-2 R1 already require that the configuration of operating systems, firmware, and software be carefully tracked such that counterfeit operating systems, firmware, software, and patches would be identified (e.g. a software difference would be identified as a change from the existing baseline configuration) and would be evaluated.

• CIP-013-1 R3.4 requires authentication of patches, updates, and upgrades, but CIP-007-6 R2.1 already imposes a patch management process for tracking, evaluating, and installing cyber security patches, including the identification of patching sources. Part of the identification of patching sources under CIP-007-6 is the verification that those sources are authentic as CIP-013-1 R3.4 would appear to require.

• CIP-013-1 R4.1 requires authorization of remote access to certain BES Cyber Systems by the vendor. CIP-004-5 R4.1.1 already contains a process for authorizing electronic access to these assets by all personnel, including vendors.

• CIP-013-1 R4.2 requires logging and monitoring or remote access sessions. CIP-007-6 R4.1 already requires logging of all access and CIP-007-6 R4.2 requires alerting for any malicious code as well as any "security ecent that the Responsible Entity determines necessitates an alert."

• CIP-013-1 R4.3 also requires responding to detected unauthorized activity, and because unauthorized activity on a BES Cyber System would constitute a "Cyber Security Incident," CIP-008-5 already requires a response to such incidents.

• CIP-013-1 R5 requires a process for controlling vendor remote access to low impact BES Cyber Systems. This overlaps with CIP-003-6 Attachment 1 Section 3 which already requires electronic access controls for low impact BES Cyber Systems the limit access to necessary access.

The draft CIP-013-1 requirements should be modified so that overlaps are removed and that CIP-013-1 only addresses vendor issues not covered within existing Standards. To the extent the SDT believes there is no overlap between CIP-013 and the existing CIP Standards, the SDT should explain in each instance where the CIP-013 Requirement ends and the other CIP Requirement begins. In the absence of such guidance, a Compliance Monitoring and Enforcement Process could conclude that a particular instance of non-compliance with CIP-013 is also a simultaneous violation of another Reliability Standard, doubling the available penalty range. For example, draft CIP-013-1 R4 requires the Responsible Entity to authorize remote access by vendor personnel. The current CIP-004-6 R4.1.1 also requires authorization of vendor personnel to have electronic access. Therefore noncompliance with CIP-013-1 R4 would appear to, per se, constitute noncompliance with CIP-004-6 R4.1.1. Such double jeopardy serves no apparent

reliability purpose. If the current CIP-013-1 R4 language is adopted as-is, the SDT should explain how its requirements differ from those under CIP-004-6 R4.1.1.

Finally, Exelon suggests that R4.3 may be difficult to accomplish in all cases and is overly prescriptive and thus should be removed from CIP-013. Order No. 829, P.52 references the Ukraine event and the threat that "vendor credentials could be stolen and used to access a BES Cyber System without the responsible entity's knowledge, as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a responsible entity's BES Cyber System." There are alternate methods to address this threat. First, two factor identification methods can be used to mitigate the risk of stolen credentials. Second, the use of WebEx or Skype sessions or active control of vendor access (i.e. opening a port for access only when needed) can be used to address emergent issues and reduce the need for remote persistent sessions.

Likes 0	
Dislikes 0	

Response

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining "unauthorized activity" if that is not changed to "unauthorized access".

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we must monitor every move, such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

We suggest that Requirement R4 Section 4.1 language be moved to the CIP-004 Standard. The group feels that CIP-004 Part 4.1 already handles access controls in that particular Cyber Standard. Additionally, we feel that a potential conflict may exist between CIP-013 Requirement R4 and CIP-004 Requirement R4 if this Requirement stays in its current position.

As for Section 4.2 language being moved to the CIP-007 Standard, our group feels that the CIP-007 Standard already addresses logging.

Finally, we suggest moving Section 4.3 Language to the CIP-005 Standard because, we feel that the CIP-005 Standard already addresses interactive access to BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Authorization of remote access to BES Cyber Systems (Part 4.1) is already addressed by CIP-004-6 R4 for user-initiated remote access and implicitly by CIP-005-5 R1 Part 1.3 (“Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.”) for machine-to-machine access. It should be deleted.

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx

Comment

See Comments on Requirement R4 in attached file.

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

Seminole Electric comments submitted by Michael Haff

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	No
Document Name	

Comment

R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.

The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.

Consider eliminating sub requirements 4.1 and 4.2 since they are covered in CIP-005 and CIP-007, R5 respectively. Consider addressing sub requirement 4.3 by modifying CIP-005 thus eliminating R4 from the proposed CIP-013 standard.

R4 should be moved to CIP-005 since this requirement, as written in CIP-013, only applies to vendors having remote access. This does not address other sources of remote access threats as written.

After moving to CIP-005, R4.2 should be revised to say: “Capability to detect unauthorized activity; and”

R4.3 should add the word “detected” before the term “unauthorized activity.”

For R4.2, we suggest limiting the retention period for evidence logs to 90 days to be consistent with CIP-007 R4, Parts 4.1, 4.2, and 4.3.

This would increase the scope of file integrity monitoring to Medium impact devices, some which are not capable of logging. This would discourage entities from allowing vendors to ever log in remotely, which might hinder reliability in the case of required emergency troubleshooting/support. Lack of timely support would also force entities to be non-compliant with other standards, such as other CIPs.

Remove vendor remote access from scope and only include system-to-system. Vendor remote access is already addressed in CIP-005 R2.

Suggest that this Rationale needs to be updated from “machine-to-machine” to “system-to-system.”

SDT appears to be building on top of CIP-005 R1.5; however, R4.3 says “during the remote access session,” which may not reasonable amount of time since this is a real-time action.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 5

Answer	No
Document Name	

Comment

R4 appears to be in parallel to requirements that already exist in CIP-004, CIP-005, CIP-007 and CIP-008. Basin Electric would prefer the requirements be integrated with the existing standards.

Basin Electric believes the following items will cause double jeopardy if there is a non-compliance action with the proposed R4:

R4, Part 4.1 is duplicative with CIP-004-6 R4, Part 4.1

R4, Part 4.2 is duplicative with CIP-007-6 R4, Part 4.1

R4, Part 4.3 should be taken care of by complying with CIP-005-5 Part 1.3 which requires inbound and outbound access permissions which prevent unauthorized activity.

R4, Part 4.3 “otherwise responding” should be taken care of by complying with CIP-008-5 R2.

In the context of R1–R3, the term “vendor” appears to apply to a company as stated in the rationale section. In context of R4, the same term “vendor” now appears to mean individual personnel who represent a company. Clarity is needed on who this requirement actually applies to.

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1

Answer	No
Document Name	

Comment

Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	

Comment

- The scope of CIP-013-1 R4 appears to overlap with parts of CIP-005-5R1.3, R1.5, R2.1 - 2.3; and CIP-007 R4.1, R4.2, R5.7. (Both of the CIP-007 and CIP-005 requirements apply to High and Medium BCS and associated EACMS, PACs, and PCAs). However, the logging and monitoring requirements in CIP-007-6 R4.1, 4.2 specifically cite “per Cyber Asset capability” and “after-the-fact investigations.”
    - Additionally, the CIP-013 requirement indicates “Disabling or otherwise responding to unauthorized activity during remote access sessions.” Not all technologies would have the capability of real-time cyber asset level user activity monitoring, needed to detect activity and disable sessions.
    - CIP-013 R4 does not consider the variability of cyber asset capability. Not all technologies can support cyber asset level logging.
- A definition of “unauthorized activity” is needed. Note: existing processes in CIP-004 establish authorized activity for vendors, contractors, and employees, including: training, PRA, and access management. Security controls in CIP-005 and CIP-007 enforce the limits of those authorizations. Vendors who are granted specific access rights to remotely access systems are, by definition, authorized to perform certain functions. Jump-hosts, firewalls, user accounts, and application privileges already limit activity to permitted activity.
- “Machine-to-machine vendor remote access” should be defined, or the formal definition of “Interactive Remote Access” should be modified to include machine access.
- “Monitoring” should be defined. Suggested clarification is that monitoring includes information regarding the startup and termination of the connection, but does not include the capturing of user activity during the session.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

SRP requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. SRP requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. SRP requests changing the language to “upon detected unauthorized activity”.

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	

Comment

CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	

Comment

We agree with the LPPC/APPA comments.

Likes 0	
Dislikes 0	

Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

CIP-013 R4.1 is duplicative of CIP-004 R4.3 as all persons already require authorization of electronic access to the systems in scope of this requirement. As entities will have to follow duplicate requirements in two different standards, CIP-004 and CIP-013, there is an increased likelihood of a violation.

CIP-013 R4.2, Logging, monitoring, and alerting is already covered in CIP-007 R4.1 and R4.2. An additional requirement part in CIP-007 R4 would be the most effective place to meet this FERC expectation. As entities will have to follow duplicate requirements in two different standards, CIP-007 and CIP-013, there is an increased likelihood of a violation.

CIP-013 R4.3 would be handled best as a component of CIP-007 R4 for detected inappropriate access. Alerting is already required by CIP-007 R4.2 and a simple additional step (requirement part) would require a response to the alert. The guidelines and technical basis should discuss use of intrusion prevention systems to meet this requirement without requiring significant additional compliance evidence.

Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	

I support the comments of Andrew Gallo at Austin Energy.

Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

R4 creates confusion and possible double jeopardy with other standards. Recommend modifying modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 address the FERC order No. 829.

Recommend that this Rationale needs to be updated from “machine-to-machine” to “system-to-system” for consistency

The first sentence of R2 is broader than the second sentence. The first sentence is “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems.” The second sentence is “The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):“ Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.

Request guidance. “Vendor-Initiated” could be considered a single word and not associated with the proposed definition of “vendor”.

Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to detected unauthorized activity.“

For R4.3, the “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Suggest changing to “detected unauthorized activity”.

Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

AE requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. AE requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. AE requests changing the language to “upon detected unauthorized activity”.

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	
PRPA requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access. Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. PRPA requests that the scope of R4 be limited to disabling remote access. For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. PRPA requests changing the language to “upon detected unauthorized activity”.	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.	

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AECI supports the following comments from the MRO NSRF:

“The NSRF believes the following items will cause double jeopardy if there is a non-compliance action with the proposed R4:

R4, Part 4.1 is duplicative with CIP-004-6 R4, Part 4.1

R4, Part 4.2 is duplicative with CIP-007-6 R4, Part 4.1

R4, P4.3 should be taken care of by complying with CIP-005-5. Part 1.3 of CIP-005-5 requires inbound and outbound access permissions which prevent unauthorized activity.”

Furthermore, AECI contends that the SDT should remove this requirement and address vendor remote access in the implementation of the supply chain risk management plan(s) as detailed in the requirement concepts proposed by AECI in Question 1. This concept will allow Responsible Entities to address the issue contractually with applicable vendors.

Likes 0	
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5

Answer	No
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

ALAN ADAMSON - New York State Reliability Council - 10

Answer	No
Document Name	

Comment

See NPCC comments.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

We request confirmation that vendor access does not include onsite staff augmentation contract resources. Clarification is also requested on whether "system to system" access applies to access that is "one-way" where the remote end conducts only monitoring activity and no control is possible. Can the procedure for access make distinctions for each method of monitoring each type of access, Interactive Remote, system to system with control and system to system for monitoring only? Finally, the term "unauthorized activity" is unclear. We recommend using the term "unauthorized access".

Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The rationale section in Requirement R4 speaks to “machine-to-machine vendor remote access” while the actual requirement speaks to “system-to-system remote access with a vendor”. ReliabilityFirst recommends the SDT use consistent language so that there is no confusion on terminology or definitions.

Requirement R4 mentions high and medium BES Cyber Systems, but does not include their associated Electronic Access Control and Monitoring Systems (EACMs), Physical Access Controls(PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following modifications for consideration:

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems [and if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets]. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy recommends that the drafting team consider creating a definition for the terms “vendor” and “unauthorized activity”. Without clear expectations as to what is considered unauthorized activity, and further technical guidance on how to detect this type of activity, the Responsible Entity will not be able to determine what to look for to comply with R4.2, and will not know when to disable this activity to comply with R4.3.

We request further clarification from the drafting team on what is meant by “*vendor-initiated Interactive Remote Access”.* Does this refer to access that originates from a non-Responsible Entity system? Also, does “*remote access*” apply in the instance where a non-Responsible Entity party accesses a BES Cyber System remotely to the ESP, but is originating on a network inside of the Responsible Entity’s infrastructure? Should the requirement language be revised to better categorize remote access as “external” remote access originating from a location that is not a Responsible Entity’s facility or location?

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Please consider consolidation of R4 requirements into CIP-005 instead of a separate requirement to assist REs who may utilized shared processes and systems for providing Interactive Remote Access, regardless of the origin of the remote access.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

This risk should be evaluated during the procurement and deployment of vendor products and services (CIP-013-1 R1), and mitigated as part of the CIP-005 R2, CIP-004 R4, and CIP-007 R4.

IID feels that there should be an exclusion comparable to a CIP Exceptional Circumstance (or Technical Feasibility Exception) added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.

Likes 0	
Dislikes 0	

Response

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3

Answer	No
Document Name	

Comment

This seems not to be a supply-chain issue. It would seem that NERC's intent is to wrap-up order 829 into a single standard instead of modifying the existing standards (CIP-005 Requirement 2), where necessary, to address these weaknesses.

There should *most definitely* be a feasibility exception with respect to 4.2 and 4.3.

What does 'during remote access sessions' mean in 4.3? If the session is active, it would be prudent to expect immediate termination of the connection as the Guidance suggests – responding in a timely manner. Termination during a remote access session could imply a normal, or 'timed' termination of the connection, long after an intended response to unauthorized activity would ordinarily occur.

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Thomas Foltz - AEP - 5

Answer	No
Document Name	

Comment

R4 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R1 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R4 should be rewritten to be only applicable to high and medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See APPA's, TAP's, and USI's comments.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

R1.2.6 is duplicative of R4. These requirements should be made consistent, or one of them should be deleted.

Much of R4 is already covered by CIP-005 (R1 and R2), CIP-007 (R4) and CIP-008. Requirements for a single topic should be consolidated within a single standard.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Response

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF believes the following items will cause double jeopardy if there is a non-compliance action with the proposed R4:

R4, Part 4.1 is duplicative with CIP-004-6 R4, Part 4.1

R4, Part 4.2 is duplicative with CIP-007-6 R4, Part 4.1

R4, P4.3 should be taken care of by complying with CIP-005-5. Part 1.3 of CIP-005-5 requires inbound and outbound access permissions which prevent unauthorized activity.

Remove "disable or other responding" and replace with "Response". Leave the options for response with the Register Entity.

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company strongly disagrees with the direction the proposed R4 requirement is taking, while recognizing the time constraints placed on the SDT to file a new or modified Standard addressing Supply Chain risks. As currently drafted, R4 carries significant overlap and repetition with existing CIP Standards, specifically with CIP-004-6 R4, CIP-005-5 R1, CIP-007-6 R4, and CIP-008-5 R2. "Authorization of remote access" should be deleted because in no way can you circumvent CIP-004-6 R4.1 requiring authorization of remote access to a high or medium impact BES Cyber System and there is no need to replicate that requirement again in this Standard. Additionally, CIP-005 R1.3 requires explicit access permissions and documented business justifications for all 'system-to-system' access, including vendor-initiated access. With respect to "logging and monitoring", and the detection of "unauthorized activity", we have serious concerns over the proposed language and provide that CIP-005-5 R1.5 already requires the detection of inbound and outbound malicious communications, CIP-007-6 R4 already requires the logging and controlling of access at each ESP boundary and to BES Cyber Systems, and CIP-008-5 R2 already requires response to detected Cyber Security Incidents, which includes unauthorized activity during a vendor remote access session. As drafted, a failure to comply with R4 could place a Responsible Entity in possible double jeopardy with those other requirements. Additionally, as written, R4 creates a scope expansion of the existing CIP-005-5 R1.5 currently applicable to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers to now ropes in all Medium Impact BES Cyber Systems – leaving entities (and auditors) to determine "which Standard wins?"

Based on those concerns, Southern Company recommends the complete removal of R4 from the Standard, and where additional controls not already covered in an existing Standard are directed in the FERC Order, those controls should be covered under "the plan(s)" under R1 in a similar manner as the proposed edits provided under R1.

If R4 is not removed in this manner, we provide the below edits for consideration with the following comments. In addition to the justified removal of "authorization of remote access", logging and controlling are achievable concepts due to their requirement under existing Standards and therefore should not be required again here in this Standard and removed. This leaves "methods to disable remote access sessions", which we propose moving under the main R4 for the applicable scenarios. Again, detecting and responding to "unauthorized activity" is already required under existing Standards, and should be removed from R4. If not removed, the SDT must address the discrepancy between the scope collision between the draft R4 and CIP-005-5 R1.5.

Additionally, if there is an expectation beyond the use of IDS/IPS for "detecting unauthorized activity", then we would argue that it is nearly impossible for an entity to look at a stream of 1's and 0's flowing by at a several megabits per second and determine whether there is "unauthorized activity" or not in that stream. With the difficulty in determining "unauthorized activity" in a stream of bits flying by, we respectfully recommend striking this and request the SDT to consider focusing the controls in this requirement specifically to having methods to rapidly "disable remote access" to prevent remote control of entity assets.

Modify R4 language as follows:

R4. Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall address methods to disable remote access sessions for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s). [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT supports the IRC comments and offers the following supplemental comments.

Requirement R4 is duplicative of existing requirements in CIP-004, CIP-005, CIP-007, and CIP-008. The drafting team should consider modifications to these existing standards rather than creating new requirements in a new standard. By placing these requirements in a stand-alone Standard, there is a possibility that entities may not make necessary connections to the prerequisites of some requirements (e.g., CIP-004 R2, R3) and downstream obligations of other requirements (e.g., CIP-008). ERCOT offers the following suggestions for realignment:

Requirements for electronic access authorization of vendors, including Interactive Remote Access, are addressed within CIP-004 R4, which also addresses the proper vetting and training of said vendors. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper pre-authorization requirements.

Requirements for Interactive Remote Access are already addressed within CIP-005 R2. Vendor-initiated remote access is just one example of Interactive Remote Access. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper configuration of remote access (e.g. multi-factor authentication, encryption, Intermediate System).

Requirements for system-to-system communications are already addressed within CIP-005 R1. This requirement could be added to CIP-005 R1 or as an addition to R2. The heading for Table 2 within CIP-005 can be modified to “Remote Access” in support of this. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper network controls for the system-to-system communication (e.g. ESPs, EAPs, etc.).

Requirements for logging and monitoring of access activity are addressed in CIP-007 R4. If the SDT keeps the requirement in CIP-013, the requirement should be modified to identify the logging specifications that differ from CIP-007 R4.

Requirements for response to unauthorized activity are already addressed within CIP-008. If the SDT keeps the requirement in CIP-013, the requirement should be modified to identify integration with CIP-008.

There are also several instances in the standard where language needs to be clarified. The drafting team should state whether system-to-system remote access includes “phone home” capabilities that are used for reporting of licensing, system health, and system problems. Requirement R4.1 should be clarified to specify whether it is addressing authorization of each remote access session or remote access to the vendor in whole. The drafting team should consider whether this requirement is consistent with current requirements in CIP-004 R4. The drafting team also needs to address authorization of software companies that use a “follow-the-sun” support model. Follow-the-sun is a type of global support where issues are passed around daily between work sites that are many time zones apart. Such a support increases responsiveness.

As noted with other requirements in the draft CIP-013 standard, the drafting team should address situations in which vendors will not or cannot provide the levels of service mandated by this requirement. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling to agree. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R4. NERC’s Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

Likes 0	
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant

Answer	No
Document Name	

Comment

We are in general agreement with EEI comments on this requirement.

Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Luis Rodriguez - El Paso Electric Company - 6

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	No
Document Name	

Comment

Access into the ESP is controlled for vendors the same as FTEs. That process is already outlined in other CIP requirements. If this is meant to be an alternative avenue of access outside the rest of the standards that is not clear.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

The standard should not create additional requirements for which entities are already being audited against. This creates confusion and risks the entity to being in double jeopardy for the same activity. NRECA recommends revising R4 to address the following:

R4, Part 4.1 is already covered under CIP-004-6 R4, Part 4.1

R4, Part 4.2 is already covered under CIP-007-6 R4, Part 4.1

R4, P4.3 is already covered under with CIP-005-5

Likes 0	
Dislikes 0	

Response

Val Ridad - Silicon Valley Power - 1 - WECC

Answer	No
Document Name	

Comment

- See APPA's comments, with which SVP agrees.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI's Position	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
We have questions and concerns about how R4 would be applied. Please see the associated comments in Question 9.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
This Requirement is duplicative of CIP-005-5.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	

Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 4.	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes identifying and logging unauthorized access is already covered. In CIP-005. Furthermore, SunPower believes that 4.3, disabling the threat of unauthorized access to BES Cyber Systems should be addressed through a revision to CIP-007, where controls for external access are covered.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No

Document Name	
Comment	
The NERC CIP Cyber Security Standards already have one of the most specific remote access security standard through CIP-005. Additional specifications to remote access should not be placed in a supply chain cyber security risk management Standard.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	

1) R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.

2) Recommend that this Rationale needs to be updated from “machine-to-machine” to “system-to-system” for consistency

3) The first sentence of R2 is broader than the second sentence. The first sentence is “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems.” The second sentence is “The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):“ Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.

4) Request guidance. “Vendor-Initiated” could be considered a single word and not associated with the proposed definition of “vendor”.

5) Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to *detected* unauthorized activity.“

6) The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.

Consider eliminating sub requirements 4.1 and 4.2 since they are covered in CIP-005 and CIP-007, R5 respectively. Consider addressing sub requirement 4.3 by modifying CIP-005 thus eliminating R4 from the proposed CIP-013 standard.

R4 should be moved to CIP-005 since this requirement, as written in CIP-013, only applies to vendors having remote access. This does not address other sources of remote access threats as written.

For R4.2, we suggest limiting the retention period for evidence logs to 90 days to be consistent with CIP-007 R4, Parts 4.1, 4.2, and 4.3.

This would increase the scope of file integrity monitoring to Medium impact devices, some which are not capable of logging. This would discourage entities from allowing vendors to ever log in remotely, which might hinder reliability in the case of required emergency troubleshooting/support. Lack of timely support would also force entities to be non-compliant with other standards, such as other CIPs.

Remove vendor remote access from scope and only include system-to-system. Vendor remote access is already addressed in CIP-005 R2.

SDT appears to be building on top of CIP-005 R1.5; however, R4.3 says “during the remote access session,” which may not reasonable amount of time since this is a real-time action.

Likes 0	
Dislikes 0	

Response

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick

Answer	No
Document Name	

Comment

Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No

Document Name	

Comment

Control of Interactive Remote Access to High and Medium Impact BES Cyber Systems is already required by CIP-005-5, Requirement R2. To that end, including that aspect in this Requirement is duplicative to some extent. Similarly, it could be argued that authorization of remote access is covered by CIP-004-6, Requirement R4, and logging of access is required by CIP-007-6, Requirement R4. The Standards Drafting Team should either incorporate the few remaining elements into the existing Requirements in the other CIP Standards, or rewrite this Requirement to only include the additional expectations not covered elsewhere.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC disagrees with the proposed requirement. CIP-013-1 R4 requires actions to be taken by the Responsible Entity that are outside of the supply chain context. FERC Order 829 specifically stated in paragraph 45 that the plan should address the security objectives in "the context of addressing supply chain management risks." NIST 800-53 provides a definition of supply chain that is as follows: "Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer." FERC Order 829 acknowledges this definition in paragraph 32, footnote 61. However, the SDT has chosen to identify controls in R4 that are executed only as part of the day-to-day management of BES Cyber Systems and introduce double jeopardy with existing CIP Reliability Standards.

R4 as written contains three parts to each be implemented for "(i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)."

4.1: Authorization of remote access. Electronic access to high and medium impact BES Cyber Systems, whether local or remote, and regardless of whether the individual is a vendor, is already required by CIP-004-6 R4, Part 4.1. System to system remote access must be explicitly permitted through the ESP along with documented justification according to CIP-005-5 R1, Part 1.3.

4.2: Logging and monitoring of remote access sessions: CIP-005-5 R1, Part 1.5 requires methods for detecting malicious communications for high impact BES Cyber Systems and medium impact BES Cyber Systems at Control Centers. CIP-007-6 R4, Part 4.1 requires logging of successful and failed access attempts. The applicable systems for CIP-007-6 R4, Part 4.1 includes EACMSs associated with medium and high impact BES Cyber Systems, effectively including logging that occurs at the perimeter of the ESP as well as access to the BES Cyber Systems directly. CIP-007-6 R4 additional requires monitoring of the logs.

4.3: Disabling or responding to unauthorized activity: CIP-008-5 R2 requires that entities respond to unauthorized activity according to their defined incident response plans. As a Cyber Security Incident includes any incident that "compromises, or was an attempt to compromise, the ESP…" or "disrupts, or was an attempt to disrupt, the operation of a BES Cyber System," response to any unauthorized activity (whether local or remote, physical or electronic) is already required by CIP-008-5 R2.

That said, there are gaps remaining between the existing CIP standards and the directive as specified by FERC Order 829.

As such, all controls required by CIP-013-1 R4 already exist in other CIP Reliability Standards, effectively making any non-compliance with R4 a case of double jeopardy with either CIP-004-6 R4, CIP-005-5 R1, CIP-007-6 R4, or CIP-008-5 R2, depending on the facts and circumstances of the specific compliance issue. While CIP-013-1 R4 suggests the implementation of technical security controls, it is unclear what additional controls would be implemented that are not already required by the existing CIP Standards. CIP-013-1 R4 only provides for additional paperwork, administrative burden, and double jeopardy compliance risk. As such, the standard drafting team should not create additional requirements for which entities are already being audited against and it should be removed.

That said, we do believe that addressing remote access in the supply chain context (not in the day-to-day operations context) could provide supply chain security risk management benefits. Unfortunately, the SDT has not constructed its requirement as such. Consistent with our response to question 1, we recommend that the SDT consider a plan based approach to addressing security risks in the context of the supply chain.

R4 is written in a manner that implies the Responsible Entity shall implement a separate documented process in addition to the plan specified in R1. Paragraph 45 of Order No. 829, clearly specifies this objective of vendor remote access should be applied to "The Plan" identified in the core directive in the context of addressing supply chain management risks.

(P. 45) The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

GTC recommends the SDT remove this requirement and include a security objective for vendor remote access in "The Plan" specified in R1 to align with the FERC Order. See GTC's comment for Question #1.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Authorization of Remote Access

The existing CIP-004 requirements already address authorization of vendor individuals and CIP-005 requirements address system-to-system authorization. We recommend that the SDT consider deleting Requirement R4, Part 4.1 to avoid this unnecessary overlap.

Activity v. Access

The use of “activity” in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as “escorted cyber access.” In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions. If “activity” is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they’ll be able to do it onsite. We recommend that the SDT consider changing “activity” to “access” in parts 4.2 and 4.3.

Remote Access Session Monitoring

Although the Commission mentions monitoring of third-party initiated remote access sessions, they direct that the standard “must address responsible entities’ logging and controlling all third-party (i.e., vendor) initiated remote access sessions.” (Order No. 829, P51) The security objective is to address “the threat that vendor credentials could be stolen and used to access a BES Cyber System without the responsible entity’s knowledge, as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a responsible entity’s BES Cyber System.” (Order No. 829, P 52).

First, the CIP-005 two factor authentication requirement would prevent access via stolen vendor credentials, except for in a sophisticated “Charles Angels” style attack (2000 movie) designed to overcome multifactor authentication, which was not the case in the Ukraine attack.

Second, monitoring remote access sessions to detect unauthorized activity is a method to control unwanted access or a “how” to implement the security objective. There are other methods to address the security objective, including controlled log-in and log-outs for specific activities and limiting the vendor’s ability to access BES Cyber Systems.

Third, session monitoring of system to system activity, as prescribed by the proposed standard is not practical due to technology constraints and the likelihood that time sensitive network traffic supporting reliability tasks could be adversely impacted. For example, where a 2 millisecond response is required in an energy management system and continuous monitoring of remote vendor access reduces system response time to 5 milliseconds. Also, technology constraints may prevent Responsible Entities from determining whether a vendor or an employee is accessing the BES Cyber System. These complications may force Responsible Entities from disallowing remote access by vendors, which may actually harm reliability rather than improve it. Vendors know their systems best since they designed and manufactured them and therefore they are in the best position for remote access to complete certain tasks.

To address the concerns, we recommend that the SDT consider changing the “monitoring” language to “control” and focus on the second part of the security objective, controlling persistent machine-to-machine remote access sessions by vendors. Controlling persistent machine-to-machine remote access is possible by different methods, including one way communications and time limiting access sessions. Vendor Interactive Remote Access is already controlled by CIP-005 requirements.

Disabling/Responding to Unauthorized Activity

Disabling remote access (Part 4.3) may also not be possible and would likely force Responsible Entities to disallow vendor remote access. We recommend that the SDT remove this part.

Requirement Placement (CIP-005)

Because Requirement R4 is an operational control, we recommend that the SDT consider putting this requirement into CIP-005 R2 and not create duplicative requirements.

Definitions

Machine-to-machine or system-to-system remote access is also not defined so it’s unclear what new systems this brings into scope for this requirement. If the SDT uses one of these terms, we recommend that they define it. Also, if the SDT uses our suggestion for addressing persistent, machine-to-machine remote access, we also recommend defining persistent, perhaps leveraging the concept used by the transient cyber asset definition. We also recommend that the SDT consider defining vendor, for example, does it include an ISO ICCP connection to an EMS?

We recommend the following language for consideration by the SDT:

R4. Each Responsible Entity shall implement one or more documented method(s) to control persistent, machine-to-machine remote access sessions by vendors to high and medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No

Document Name	
Comment	

The IRC and SWG request that the SDT consider moving this requirement to existing CIP Standard to prevent overlap, conflict, or omission of existing requirements.

The SDT should address whether system-to-system access is when vendor-initiated. Lack of clarity there will impact automated updates from vendors that are time-sensitive, as well as outbound connections to vendors for health checks, licensing, and other system information.

Likes 0	
Dislikes 0	
Response	

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	
Comment	

Authorization of Remote Access

The existing CIP-004 requirements already address authorization of vendor individuals and CIP-005 requirements address system-to-system authorization. We recommend that the SDT consider deleting Requirement R4, Part 4.1 to avoid this unnecessary overlap.

Activity v. Access

The use of “activity” in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as “escorted cyber access.” In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions. If “activity” is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they’ll be able to do it onsite. We recommend that the SDT consider changing “activity” to “access” in parts 4.2 and 4.3.

Remote Access Session Monitoring

Although the Commission mentions monitoring of third-party initiated remote access sessions, they direct that the standard “must address responsible entities’ logging and controlling all third-party (i.e., vendor) initiated remote access sessions.” (Order No. 829, P51) The security objective is to address “the threat that vendor credentials could be stolen and used to access a BES Cyber System without the responsible entity’s knowledge, as well as the

threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a responsible entity's BES Cyber System." (Order No. 829, P 52).

First, the CIP-005 two factor authentication requirement would prevent access via stolen vendor credentials, except for in a sophisticated "Charles Angels" style attack (2000 movie) designed to overcome multifactor authentication, which was not the case in the Ukraine attack.

Second, monitoring remote access sessions to detect unauthorized activity is a method to control unwanted access or a "how" to implement the security objective. There are other methods to address the security objective, including controlled log-in and log-outs for specific activities and limiting the vendor's ability to access BES Cyber Systems.

Third, session monitoring of system to system activity, as prescribed by the proposed standard is not practical due to technology constraints and the likelihood that time sensitive network traffic supporting reliability tasks could be adversely impacted. For example, where a 2 millisecond response is required in an energy management system and continuous monitoring of remote vendor access reduces system response time to 5 milliseconds. Also, technology constraints may prevent Responsible Entities from determining whether a vendor or an employee is accessing the BES Cyber System. These complications may force Responsible Entities from disallowing remote access by vendors, which may actually harm reliability rather than improve it. Vendors know their systems best since they designed and manufactured them and therefore they are in the best position for remote access to complete certain tasks.

To address the concerns, we recommend that the SDT consider changing the "monitoring" language to "control" and focus on the second part of the security objective, controlling persistent machine-to-machine remote access sessions by vendors. Controlling persistent machine-to-machine remote access is possible by different methods, including one way communications and time limiting access sessions. Vendor Interactive Remote Access is already controlled by CIP-005 requirements.

Disabling/Responding to Unauthorized Activity

Disabling remote access (Part 4.3) may also not be possible and would likely force Responsible Entities to disallow vendor remote access. We recommend that the SDT remove this part.

Requirement Placement (CIP-005)

Because Requirement R4 is an operational control, we recommend that the SDT consider putting this requirement into CIP-005 R2 and not create duplicative requirements.

Definitions

Machine-to-machine or system-to-system remote access is also not defined so it's unclear what new systems this brings into scope for this requirement. If the SDT uses one of these terms, we recommend that they define it. Also, if the SDT uses our suggestion for addressing persistent, machine-to-machine remote access, we also recommend defining persistent, perhaps leveraging the concept used by the transient cyber asset definition. We also recommend that the SDT consider defining vendor, for example, does it include an ISO ICCP connection to an EMS?

We recommend the following language for consideration by the SDT:

R4. Each Responsible Entity shall implement one or more documented method(s) to control persistent, machine-to-machine remote access sessions by vendors to high and medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

This requirement is duplicative of existing requirements within CIP standards.

Authorization of access is covered in CIP-004-6 R4.1. The language in this CIP-004-6 R4.1 does not exclude vendors.

The rationale for CIP-007-6 R4 explicitly states that security event monitoring's purpose is to detect unauthorized activity.

A detection of unauthorized activity would be investigated as a potential Cyber Security Incident and appropriate action would be taken from there.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC

Answer	No
Document Name	

Comment

SDG&E agrees with EEI comments and proposed language. These operations requirements are covered in other CIP standards.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	

Comment

Tacoma concurs with the comments provided by the LPPC.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Authorization of Remote Access

The existing CIP-004 requirements already address authorization of vendor individuals and CIP-005 requirements address system-to-system authorization. We recommend that the SDT consider deleting Requirement R4, Part 4.1 to avoid this unnecessary overlap.

Activity v. Access

The use of “activity” in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as “escorted cyber access.” In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions. If “activity” is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they’ll be able to do it onsite. We recommend that the SDT consider changing “activity” to “access” in parts 4.2 and 4.3.

Remote Access Session Monitoring

Although the Commission mentions monitoring of third-party initiated remote access sessions, they direct that the standard “must address responsible entities’ logging and controlling all third-party (i.e., vendor) initiated remote access sessions.” (Order No. 829, P51) The security objective is to address “the threat that vendor credentials could be stolen and used to access a BES Cyber System without the responsible entity’s knowledge, as well as the

threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a responsible entity's BES Cyber System." (Order No. 829, P 52).

First, the CIP-005 two factor authentication requirement would prevent access via stolen vendor credentials, except for in a sophisticated "Charlie's Angels" style attack (2000 movie) designed to overcome multifactor authentication, which was not the case in the Ukraine attack.

Second, monitoring remote access sessions to detect unauthorized activity is a method to control unwanted access or a "how" to implement the security objective. There are other methods to address the security objective, including controlled log-in and log-outs for specific activities and limiting the vendor's ability to access BES Cyber Systems.

Third, session monitoring of system to system activity, as prescribed by the proposed standard is not practical due to technology constraints and the likelihood that time sensitive network traffic supporting reliability tasks could be adversely impacted. For example, where a 2 millisecond response is required in an energy management system and continuous monitoring of remote vendor access reduces system response time to 5 milliseconds. Also, technology constraints may prevent Responsible Entities from determining whether a vendor or an employee is accessing the BES Cyber System. These complications may force Responsible Entities from disallowing remote access by vendors, which may actually harm reliability rather than improve it. Vendors know their systems best since they designed and manufactured them and therefore they are in the best position for remote access to complete certain tasks.

To address the concerns, we recommend that the SDT consider changing the "monitoring" language to "control" and focus on the second part of the security objective, controlling persistent machine-to-machine remote access sessions by vendors. Controlling persistent machine-to-machine remote access is possible by different methods, including one way communications and time limiting access sessions. Vendor Interactive Remote Access is already controlled by CIP-005 requirements.

Disabling/Responding to Unauthorized Activity

Disabling remote access (Part 4.3) may also not be possible and would likely force Responsible Entities to disallow vendor remote access. We recommend that the SDT remove this part.

Requirement Placement (CIP-005)

Because Requirement R4 is an operational control, we recommend that the SDT consider putting this requirement into CIP-005 R2 and not create duplicative requirements.

Definitions

Machine-to-machine or system-to-system remote access is also not defined so it's unclear what new systems this brings into scope for this requirement. If the SDT uses one of these terms, we recommend that they define it. Also, if the SDT uses our suggestion for addressing persistent, machine-to-machine remote access, we also recommend defining persistent, perhaps leveraging the concept used by the transient cyber asset definition. We also recommend that the SDT consider defining vendor, for example, does it include an ISO ICCP connection to an EMS?

We recommend the following language for consideration by the SDT:

R4. Each Responsible Entity shall implement one or more documented method(s) to control persistent, machine-to-machine remote access sessions by vendors to high and medium impact BES Cyber Systems.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of

Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	

SMUD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. SMUD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. SMUD requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	
Response	
Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	

The NYPA Comments	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	CIP-013 Comment Mar 2 revision SCL 2017-3-6.docx
Comment	

The attached document has comments compiled for all the questions. Please note that the BOLD paragraphs below (YELLOW highlighted in attachment) are uniquely Seattle City Lights. The un-highlighted comments were developed in collaboration with other entities and trade organizations such as LPPC. These comments may be like those submitted by other entities but not necessarily. City Light recognizes the challenges facing the SDT and appreciates the efforts the SDT is placing into working towards developing a solid standard.

Seattle City Light requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. Seattle City Light requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Seattle City Light requests changing the language to "upon detected unauthorized activity".

Furthermore, because it may not be technically feasible to remotely disable a vendor from equipment provided by that vendor (which the entity purchased from them, and may be dependent upon the vendor for maintenance), Seattle City Light requests the inclusion of a Technical Feasibility Exception (TFE) for R4. Seattle City Light suggests the following language: "WHERE TECHNICALLY FEASIBLE, each responsible entity shall implement one or more documented process(es) for controlling vendor remote access to…" (emphasis added).

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

The IESO request that the SDT consider moving this requirement to existing CIP Standard to prevent overlap, conflict, or omission of existing requirements.

The SDT should address whether system-to-system access is when vendor-initiated. Lack of clarity there will impact automated updates from vendors that are time-sensitive, as well as outbound connections to vendors for health checks, licensing, and other system information.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities

Answer	No
Document Name	

Comment

Colorado Springs Utilities (CSU) requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. CSU requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CSU requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry

Answer	No
Document Name	

Comment

See EEI comments

Likes 0	
Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	

1) R4 creates confusion and possible double jeopardy with other standards. Recommend modifying modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 address the FERC order No. 829.

2) For R4.3, the “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Suggest changing to “detected unauthorized activity”.

3) Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA believes the scope should be limited to High and Medium BES cyber systems with ERC or dialup. All requirements for Low impact systems should be addressed in CIP-003.

BPA suggests modification of existing CIP standards to address gaps:

Remote access CIP-013 R4, P4.1 is addressed in CIP-004-6 R4, Part 4.1

Logging and monitoring CIP-013 R4, P4.2 is addressed in CIP-007-6 R4, P4.1

Remote access sessions CIP-013 R4, P4.3 is addressed in CIP-005 R2

Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	

This requirement is duplicative of existing requirements within CIP standards.

Authorization of access is covered in CIP-004-6 R4.1. The language in this CIP-004-6 R4.1 does not exclude vendors.

The rationale for CIP-007-6 R4 explicitly states that security event monitoring's purpose is to detect unauthorized activity.

A detection of unauthorized activity would be investigated as a potential Cyber Security Incident and appropriate action would be taken from there.

Likes 0	
Dislikes 0	
Response	

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Santee Cooper requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. Santee Cooper requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Santee Cooper requests changing the language to "upon detected unauthorized activity".

Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
Rationale for Requirement R4: The rationale language for R4 states, “The proposed requirement addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51).” R1, R2, and the Rationale for Requirement R3 and R4 do not specify the impact classifications (High, Medium and Low) when referencing the BES Cyber System. R3 and R4 specifically state the impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems (R3)” or “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems (R4).” IPC would like to know if the inconsistent impact classification references were intended or were an oversight by the SDT? **R4** IPC does not believe CIP-013-1 is an appropriate standard to address R4.1, R4.2 and R4.3. IPC believes R4.1 belongs in CIP-004-6, as R4.1 is related to authorization and R4.2 and R4.3 belongs in CIP-005-6 as R4.2 and R4.2 are related to remote access. IPC feels the intent of CIP-013-1 is to address supply chain controls, whereas CIP-004-6 addresses access management and CIP-005-6 addresses remote access. **M4** Some of the measure language for R4 states, “hard copy or electronic listing of alert capabilities applicable to vendor remote access of the BES Cyber System; or records of response to unauthorized vendor remote access.“ R1, R2, and the Rationale for Requirement R3, R4, and M4 do not specify the impact classifications (High, Medium and Low) when referencing the BES Cyber System. R3 and R4 specifically states the impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems (R3)” or “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems (R4).” IPC would like to know if the inconsistent impact classification references were intended or were an oversight by the SDT?

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	

Comment
Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016. Reclamation recommends that Requirement R4 be deleted. There would be no need for Requirement R4 if all aspects of the supply chain risk management plan(s) are to be addressed in Requirement R1 and its sub-requirements.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	No
Document Name	
Comment	
1. As mentioned above, the standard drafting team should not create additional requirements for which entities are already being audited against. This creates confusion and risks the entity to being in double jeopardy for the same activity. R4, Part 4.1 is covered under CIP-004-6 R4, Part 4.1 R4, Part 4.2 is covered under CIP-007-6 R4, Part 4.1 R4, P4.3 is covered under with CIP-005-5. Part 1.3 of CIP-005-5	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

Requirement R4:

ATC agrees with the value provided through the implementation of controls to address logging and controlling third-party initiated remote access; however, ATC has voted “No” to the proposed language developed CIP-013-1 Requirement R4 because existing Reliability Standards accomplish this objective rendering the need for this requirement in CIP-013-1 moot. In its redundancy, it is at odds with the former efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

Requirement R4 Sub Requirement 4.1 – 4.3:

CIP-013-1 R4 is simultaneously duplicative and additive to the language and/or intent of several existing approved and effective CIP Cyber Security Reliability Standards and is therefore providing no additional security or reliability value and creating a condition of double jeopardy for Registered Entities where a violation of CIP-013-1 R4 would constitute a violation of another CIP Standard and requirement.

CIP-004-6 R4 and R5 address access management and revocation for individuals having cyber access to specified high and/or medium impact-rated BES Cyber Systems and associated Cyber Assets. The existing enforceable CIP-004-6 standard is silent to the capacity with which a given individual is engaged with a Registered Entity, and therefore in its silence it addresses employees, contractors, interns, apprentices, or even vendors etc. These access requirements within CIP-004-6 are more prescriptive than what is proposed for CIP-013-1 therefore providing no additional security or reliability value and ultimately rendering CIP-013-1 R4.1 superfluous and unnecessary.

CIP-005-5 R1 Parts 1.1 – 1.4 addresses CIP-013-1 R4(i), R4.1, ultimately rendering CIP-013-1 R4(i), R4.1 superfluous and unnecessary in that:

- CIP-005-5 R1 Parts 1.3 mandates authorization for system-to-system remote access through the requirement for inbound and outbound access permissions through an identified Electronic Access Point protecting high and/or medium impact-rated BES Cyber Systems,
  - where those BES Cyber Systems must already be protected as a function of being inside an identified Electronic Security Perimeter pursuant to CIP-005-5 Requirement R1 Part 1.1, and
  - where all External Routable Connectivity must be through an identified Electronic Access Point pursuant to CIP-005-5 Requirement R1 Part 1.2.
- Additionally, CIP-005-5 R1 Part 1.4 obligates Registered Entities to perform authentication for establishing Dial-up connections to high and/or medium impact-rated BES Cyber Systems, where technically feasible. The broad reference to system-to system remote access (which is silent to Dial-up) in combination with the absence of the provision for technical feasibility within this draft Requirement is effectively and expansion in scope to the already approved and enforceable CIP-005-5 R1 Part 1.4 Reliability Standard. Any expansion in scope to remote access requirements or controls for high or medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-005-5 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the

creation of a separate one. Furthermore, it is a contradiction between standards where compliance with one requirement in CIP-005-5 R1 Part 1.4 through a CIP Senior Manager and regional regulator approved Technical Feasibility Exception becomes a matter of non-compliance pursuant to CIP-013-1 R4.

CIP-005-5 R2 Parts 2.1 – 2.3 and CIP-007-6 R5 Parts 5.1 goes beyond in addressing CIP-013-1 R4(ii), R4.1, ultimately rendering CIP-013-1 R4(ii), R4.1 superfluous and unnecessary in that:

- CIP-005-5 R1 Parts 2.1 mandates authorization for all Interactive Remote Access (IRA) (including vendor-initiated IRA) through the requirement to use an Intermediate System such that any remotely-initiated IRA does not directly access the high and/or medium impact-rated BES Cyber System(s),
- where those Intermediate System must also utilize encryption that terminates at the Intermediate System pursuant to CIP-005-5 Requirement R2 Part 2.2, and
- where all IRA sessions must require multi-factor authentication pursuant to CIP-005-5 Requirement R2 Part 2.2.
- CIP-007-6 R5 Parts 5.1 further mandates methods to enforce authentication of interactive user access (including vendor-initiated users) where technically feasible for high and/or medium impact-rated BES Cyber System(s),

CIP-005-5 R1 Parts 1.2 - 1.5, in combination with CIP-007-6 R4 Parts 4.1-4.4 and CIP-007-6 R5 Part 5.7 collectively addresses, and in some cases exceeds, the logging, monitoring, and detection of unauthorized activity proposed in CIP-013-1 R4, R4.2, ultimately rendering in CIP-013-1 R4, R4.2 superfluous and unnecessary in that:

- CIP-005-5 R1 Part 1.5 mandates one or more methods for detecting known or suspected malicious communications both inbound and outbound on the Electronic Access Points protecting high and/or medium impact-rated BES Cyber System(s), and because all remote access must also be through an identified Electronic Access Point pursuant to CIP-005-5 Requirement R1 Part 1.2, the two existing enforceable requirements in combination already satisfying the detection component intended by CIP-013-1 R4, R4.2; and consequently, the detection component intended by CIP-013-1 R4, R4.2 adds no security or reliability value and rather creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-005-05 R1.
- CIP-007-6 R4 Parts 4.1-4.4 mandates that, per BES Cyber System capability or at the Cyber Asset level for high and/or medium impact-rated BES Cyber System(s),
  - specified access-related events are logged,
  - alerts are generated for said events,
  - event logs are retained as technically feasible for 90 consecutive calendar days except in CIP Exceptional Circumstances,
  - thereby already satisfying the logging and monitoring component intended by CIP-013-1 R4, R4.2; Consequently, the logging and monitoring component intended by CIP-013-1 R4, R4.2 adds no security or reliability value and rather creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-007-6 R4 that is also at odds with efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.
  - Furthermore, in its redundancy of CIP-007-6 R4, CIP-013-1 R4, R4.2 is simultaneously an expansion in scope in that CIP-013-1 R4, R4.2 is silent to the provisions for “Per Cyber System capability”, per cyber Asset capability”, “technical feasibility”, and “CIP Exceptional Circumstances”, is effectively and expansion in scope to the already approved and enforceable CIP-007-6 R4 Reliability Standard. Any expansion in scope to logging, monitoring, or detection activity related to requirements or controls for high or medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-007-6 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one. Furthermore, it is a contradiction between standards where compliance with one requirement in CIP-007-6 R4 through:

- a CIP Senior Manager and regional regulator approved Technical Feasibility Exception,
- a CIP Senior Manager approved CIP Exceptional Circumstance,
- a documented per BES Cyber System incapability, and/or
- a documented per Cyber Asset incapability

becomes a matter of non-compliance pursuant to CIP-013-1 R4.2

- CIP-007-6 R5 Part 5.7 mandates limiting of the number of unsuccessful authentication attempts or the generation of alerts of unsuccessful authentication attempts exceeding a Registered Entity defined threshold, where technically feasible and scope to high impact BES Cyber Systems and medium impact BES Cyber Systems at Controls Centers. The broad reference high and medium impact BES Cyber Systems, in combination with the absence of the provision for technical feasibility within this draft Requirement for CIP-013-1 R4 is effectively and expansion in scope to the already approved and enforceable CIP-007-6 R5.7 Reliability Standard. Any expansion in scope to logging, monitoring, or detection activity related to requirements or controls for high or medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-007-6 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one. Furthermore, it is a contradiction between standards where compliance with one requirement in CIP-007-6 R5 Part 5.7 through a CIP Senior Manager and regional regulator approved Technical Feasibility Exception becomes a matter of non-compliance pursuant to CIP-013-1 R4.

Likes 0	
Dislikes 0	

Response

Ballard Mutters - Orlando Utilities Commission - 3

Answer	No
Document Name	

Comment

OUC requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. OUC requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. OUC requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
The Technical Guidance and Examples state that “for Requirement R4 Part 4.1, an entity may already have some authorization controls in place that will support meeting this objective”, including CIP-004 and CIP-007 R5 controls if they are fully implemented for vendor-initiated Interactive Remote Access. Please confirm that implementation of these controls for all remote access, vendor or entity initiated, would meet compliance with this requirement. If so, would it be beneficial to caveat the requirement and have it read “**4.1** Authorization of remote access, not previously approved by CIP-004, by the Responsible Entity?” A responsible entity may have numerous contractors from various vendors that perform a number of tasks within CIP environments that are on-site, sitting right next to employees engaged in similar activities. Both the contractors and the employees normal work process may have them utilize Interactive Remote Access to perform their responsibilities efficiently. Are these contractors, embedded and onsite, to have each of their connections explicitly approved and monitored at a different level of scrutiny than actual employees of the responsible entity, simply because they are not employees? Or will there be a distinction between on-site and off-site “vendors?”	
Likes 0	
Dislikes 0	

Response
Steven Rueckert - Western Electricity Coordinating Council - 10
Answer	Yes
Document Name	
Comment
R4 could give entities the impression that they do not need to follow the CIP-005-5 R2 controls for Interactive Remote Access. If an entity did not leverage its existing Interactive Remote Access (CIP-005-5 R2) processes to support this Requirement, WECC is concerned that separate vendor remote access processes may provide additional ingress/egress points into the ESP. An entity should ensure that vendor remote processes are protected at least to the level of CIP-005-5 R2. At no point in time, should there ever be an unmonitored connection into a BCS. This is something that is totally under the control of the entity. Even if the vendor includes a "phone-home" feature on a system or application, the ingress and egress of that connection should still be monitored and controlled by the entity to minimize the risk of third-party penetration into the BCS. The SCRM team should work closely with the CIP-005-5 team to ensure all remote access connections are managed, monitored, and controlled through an Electronic Access Control and Monitoring System [EACMS] and/or Intermediate System [IS]
Likes 0	
Dislikes 0	
Response
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable
Answer	Yes
Document Name	
Comment
While in overall agreement with this Requirement R4, ACEC would recommend the following change: 1. Move Requirement 1, Part 1.2.2, "Process(es) for notification when vendor employee remote or onsite access should no longer be granted" and Part 1.2.6 "Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)" to Requirement R4 since this requirement is where Vendor Remote Access is addressed.
Likes 0	
Dislikes 0	
Response
Rachel Coyne - Texas Reliability Entity, Inc. - 10
Answer	Yes
Document Name	

Comment
This appears to meet the FERC directive.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment
No additional comments.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	

Comment
We recommend the SDT address CIP Exceptional Circumstance with respect to this requirement aligned with project 2016-02. Also please see our earlier comments with regards to redundancy between R4 and R1.2.6.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment
PSEG agrees with the intent of this requirement, but has the following questions/recommendations below: • Recommend changing Requirement 4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to detected unauthorized activity associated with remote access sessions.“ PSEG finds that inclusion of the word “during” in the requirement overreaches the intent of relevant FERC directive (p.51). • Requirements R1 and R2 do not require the registered entity to go back and revise previous contracts. In order to comply with this requirement, R4, past contracts / vendor service agreements may be required. Alignment is needed between R1, R2, and R4. • Vendor-initiated Interactive remote access is no different than Interactive remote access. Recommendation to incorporate Requirement R4 into CIP-007 R5 System Access Control. • Requirement R4 overlaps with CIP-005 for Interactive Remote Access, which applies to vendors, only 4.2 monitoring and 4.3 is new. Recommend streamlining R4 to fit in CIP-005 R2. • Recommend changing “activity” to “access”. Use of the word “activity” in 4.2 and 4.3 because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. In almost all cases, the vendor has more in depth technical knowledge of the system they developed beyond the Registered Entity’s level of expertise on the system. Therefore it would be difficult for the Responsible Entity to recognize inappropriate actions/activity. If “activity” is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they’ll be able to do it onsite. If the intent of this requirement is to monitor “unauthorized activity”, the term “unauthorized activity” should be defined.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	

Comment
AZPS requests changing Requirement R4.3 to read ‘disabling or otherwise responding to **detected,** unauthorized activity during remote access session’. It further notes that, as written, the proposed Requirement R4 would place Registered Entities in “double jeopardy” where similar controls are already required under CIP-004-6. Accordingly, AZPS requests that the SDT consider revising this requirement to remove such redundancy or to include a clarification regarding how this risk for “double jeopardy” will be managed relative to access controls required under CIP-004-6.

Likes 0	
Dislikes 0	

Response

John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wes Wingen - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
George Tatar - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	

Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	

Refer to CSU comments.	
Likes 0	
Dislikes 0	
Response	

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF does not understand the intent of the following:

R1 is applicable to “Each Responsible Entity” is to implement “one or more supply chain risk management plans”.

R2 is applicable to “Each Responsible Entity” is to review and update its “supply chain risk management plans” at least once every 15 calendar months.

R5 is applicable to “Each Responsible Entity” with at least one “low impact BES Cyber System” will have a documented “cyber security policies “ which require “review and approval” at least once every 15 calendar months.

For R5.1, imposes a requirement at the BES Cyber Asset level rather than at the BES Cyber System level. Consider removing R5.1 or reworking so it is applicable at the BES Cyber System level.

The NSRF has concerns with R5. As written, every entity with a “low impact BES Cyber System” is required to have “cyber security policies” (note policies should be changed to “policy(s)). This would include entities that have High and Medium impact BES Cyber Systems, as long as they have one “low impact BES Cyber System”, too. Plus, R5.1 is a duplicate of R3 and R5.2 is a duplicate of R1.2.6.

This will cause double jeopardy for Each Responsible Entity in R1, R2, and R5. The “Responsible Entities” statement within each Requirement contains “High, Medium, and Low BES Cyber Systems”. So everywhere “Responsible Entity” is used in the Standard, that requirement applies to everyone with High, Medium, and Low BES Cyber Systems.

The NSRF believes that this is NOT the intent of R5. If the intent of R5 is to have control for Entities with “low impact BES Cyber Systems” **only** then, it should be clearly stated. Such as:

*“R5. Each Responsible Entity with at least one asset identified in CIP-002, containing low impact BES Cyber Systems **only,** shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:”*

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
Requirement 5.1 needs to be removed. Currently patching is not required as a function for low impact assets. Until vulnerability and patching is made a requirement for low impact assets, then it is not possible to ensure that “all” patches for low impact assets be validated for authenticity. Additionally, given the issues with trying to validate authenticity for software and patches in general (see our comments on R3) then this sub-requirement cannot be enforced. The sub-requirement for remote access is valid and should be implemented for low impact assets.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The standard as written doesn’t clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
R5 requires a Policy for Low Impact BES Cyber Systems. The two sub requirements are more plan based than policy based and would recommend making them an addition to CIP-003-7(i) attachment A instead. This will keep all LOW Impact BES Cyber Asset requirements in one location.	
Likes 0	

Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	

Comment
R5 fundamentally does not work as a low-impact scale-back of R3 and R4, because it can be meaningfully implemented only on a Cyber Asset level, and CIP-002-5.1 (R1.1.3) and CIP-003-6 (R2) do not require identification of Cyber Assets for low-impact BES Cyber Systems. The entire concept of R5 needs revision. The difference between supply chain risk management policies, as called-for in R5, and processes, mandated in R3 and R4, is unclear. TFE opportunity is again needed, nor should there be any obligation to impose measures on vendors (see our “additional comments” responses).

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	

Comment
See APPA's, TAP's, and USI's comments.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 5	
Answer	No
Document Name	

Comment

AEP is concerned about low impact BES Cyber Systems being included here because it may incentivize a lack of action on those systems in order to avoid compliance obligations. AEP believes the Standard should be reasonable for all to achieve, and this may create a significant recordkeeping burden for low impact systems. R5, as proposed, only requires a “documented policy”. Responsible entities could manage the risk appropriately for their circumstances without a requirement to “implement”.

Likes 0	
Dislikes 0	

Response

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3

Answer	No
Document Name	

Comment

See comments to Question 1.

These should clearly be modifications to CIP-003-7(i) Attachment A, and not lumped into CIP-013, Supply Chain Risk Management.

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

These risks should be evaluated during the procurement and deployment of vendor products and services (CIP-013-1 R1), and mitigated as part of the CIP-005 R2 and CIP-007 R2.

IID does not agree with including Low Impact BES Cyber Systems in this standard as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. As written, this requirement will place additional administrative burden on entities and the impacts are not fully understood. The SDT would need to clarify measures that would serve as evidence. As mentioned above, if the SDT feels that gaps remain, SRP feels that the modifications should be made in the standard where the topic is already addressed (CIP-003).

Additionally, IID feels that there should be exclusion comparable to a CIP Exceptional Circumstance (or TFE) added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The current CIP requirements for BCS at low impact sites do not require identification of patch sources, or other patching procedural controls. Introducing R5 inadvertently requires utilities to develop a CIP-007 R2 program for low sites as well to be able to address software integrity. This policy would also require a software list and inventory of systems to provide evidence that the policy has been followed. Implementing CIP-013 essentially applies controls from CIP-005, CIP-007, CIP-008, and CIP-010 to BCS at low impact sites where there are no corresponding requirements within the existing CIP standards. For example, it is incongruous to require verification of patches on a low BCS for which there is no requirement to patch.	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	No
Document Name	
Comment	
Smaller generation facilities are heavily dependent on the Original Equipment Manufacturers, and do not have the leverage to promote participation from large sole sources. How do facilities develop processes to verify integrity and authenticity of software and firmware, when OEMs don't offer guidance on validation? The sole sources also do not have the incentive to adhere to the same level of compliance when these assets are in their care, such as when embedded cyber assets are shipped off site to the OEM, or when service engineers are on site for commissioning. Enhanced compliance requirements discourages equipment servicing from the owner, and places more reliance on the OEM.	
Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy recommends the deletion of this requirement. As stated in our comments earlier, based on the minimal threat to stability that Low Impact BES Cyber Systems pose to the BES, coupled with the lack of an inventory list for said Low Impact systems to demonstrate compliance, we feel that this requirement is unnecessary and impossible to effectively demonstrate compliance to.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

Requirement R5 speaks to documenting a policy or policies to address 5.1 and 5.2 for low impact BCS. The word “implement” is not in this requirement. Absent including the implementation piece, there is no requirement to implement the controls just document them.

Furthermore, the SDT made it clear in Requirement R3 and R4 that an entity shall implement one or more documented process(es) for the actual security controls or processes. Similar language (implement documented process(es)) should be included in R5 versus policy. Even though the rationale section speaks to policies and processes, the language of the requirement only speaks to policies. This will drive consistent implementation across all BCS impact levels. ReliabilityFirst offers the following modifications for consideration to address our concern:

R5. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall [implement] have one or more documented cyber security policies [or processes], which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	

Answer	No
Document Name	

Comment

We request consistency in the use of terms between R1 and R5; R1 uses the term “plan” and R5 uses the term “process” or “policy”. We understand the term “plan” to mean a more high-level document that communicates management goals and objectives. We request clarification that the use of the term “policy” in R5 is meant to be a similar concept, i.e., that R5 is satisfied by a document that is reviewed and approved by the CIP Senior Manager that is a high-level document that communicates management goals and objectives, rather than a detailed process document with instructions to achieve the requirements. We seek this clarification because in the Technical Guidance and Examples (page 16 lines 29-31), the SDT writes “or alternatively develop a separate cyber security policy or process(es) to address low impact BES Cyber System.” As described previously by the Version 5 SDT, a documented process and a policy are two different documents: a policy is a document used to communicate management goals and objectives, while a process is a set of required instructions specific to achieving the requirement. Based on the SDT’s comments in the Technical Guidance and Examples, it is unclear which will satisfy R5 and how it will be audited.

Clarification is also requested on whether “system to system” access applies to access that is “one-way” where the remote end conducts only monitoring activity and no control is possible. Can the procedure for access make distinctions for each methods of monitoring each type of access, Interactive Remote, system to system with control and system to system for monitoring only?

Additionally, we request confirmation that if vendors refuse or can’t provide hashes or other verification methods, an internal process to test, scan and perform verification activities be enough to satisfy requirement R5.1.

Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Response

ALAN ADAMSON - New York State Reliability Council - 10

Answer	No
Document Name	

Comment

See NPCC Comments.

Likes 0	
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5

Answer	No

Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI has concerns that R5, as written, would place Responsible Entities that have a combination of High, Medium, and low impact BES Cyber Systems at risk of double jeopardy. Part 5.1 is a duplicate of R3 and R5.2 is a duplicate of R1.2.6. This requirement should be removed from CIP-013-1 and addressed in CIP-003, R2, Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	No

Document Name	
Comment	
PRPA is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. PRPA requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, PRPA requests that all requirements related to low impact assets be included in CIP-003.	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Response	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	
AE is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. AE requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, AE requests that all requirements related to low impact assets be included in CIP-003.	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No

Document Name	

Comment

The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003.

R5.1 is not consistent with R1.2.5, should R5.1 include the term “that are intended for use” to read “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and”

Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls R5 needs to be a process not a policy. If this is a policy, then suggest removing “controlling”

There should be exclusion comparable to a CIP Exceptional Circumstance added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.

If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy. R5 should be a plan document and not a policy document.

Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	No

Document Name	
Comment	
CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
CIP-013-1 R5 should be placed within CIP-003 in order to keep consistency with the approach used in the remaining CIP standards. Low impact requirements were placed in CIP-003 in order to keep all requirements within a single standard and requirement. By adding these requirements into a new standard, there is confusion resulting in an increased likelihood of a violation. Guidance language should be added for the auditing process within the standard's guidelines and technical basis (not in a separate document). Not including this in the standard places no obligation on the auditors. Without this guidance language, the auditors could choose to audit in a near zero defect manner, as opposed to a quality of program manner. Providing clear guidance sets expectations for the entities.	
Likes 0	
Dislikes 0	
Response	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Response	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. SRP requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, SRP requests that all requirements related to low impact assets be included in CIP-003.	
Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	
Response	

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	

- This Requirement should be removed from the Standard. For consistency with the other CIP Standards (e.g. compare to the current draft revision of CIP-003-7i standard where Transient Cyber Asset language for assets that contain Low Impact BCS is included) applicability of supply chain risk management to assets that contain Low Impact BCS should be consigned to CIP-003, R1.2 and R2:
    - R2 – Attachment 1 should be expanded to include a Section for supply chain risk management (to include controls on software authenticity for Low Impact BCS, controlling vendor remote access to Low Impact BCS)
    - R1.2 – should be expanded to include supply chain risk management plan(s) with controls for assets that contain Low Impact BCS
- The NERC Glossary of Terms definition of CIP Senior Manager will require update to include CIP-013

Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	

Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	

Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 5

Answer	No
Document Name	

Comment

Basin Electric would prefer low impact requirements be included in CIP-003 rather than CIP-013.

For R5.1, imposes a requirement at the BES Cyber Asset level rather than at the BES Cyber System level. Consider removing R5.1 or reworking so it is applicable at the BES Cyber System level. Basin Electric is concerned R5.1 will necessitate maintaining a list of low BES Cyber Systems and possibly a list of low BES Cyber Assets.

Basin Electric suggests modifying the requirement to include clarification of when the obligation starts. Perhaps add language to the front of R5 such as: "For assets containing low impact BES Cyber Systems in production…"

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	No
Document Name	

Comment

The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1. R5 will be the only low impact specific requirement not to be in CIP-003.

Concerned that in R5.2 the term "controlling" is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing "controlling"

CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request “per system capability” wording for R5. Not all vendors provide a “golden hash” or other mechanism to validate.
- To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.”

Does R5 allow the Entity to “accept the risk?”

R5.2 should be revised to say, “Ability to disable or otherwise respond to detected unauthorized activity during remote access sessions.”

Language of R5 should say “…shall document and implement one or more cyber security policies…” to clarify that implementation is expected for compliance. Draft R5 language does not include the term “implement”.

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

Seminole Electric comments submitted by Michael Haff

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx

Comment

See comments on Requirement R5 in attached file.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes it is inappropriate to try to define what amount to electronic access control requirements (vendor remote access) while revised electronic access control requirements in CIP-003 have not yet been formally approved.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
As we reviewed Requirement R3 and Requirement R4, it is our understanding that a Management Plan needs to be developed and maintained. However, Requirement R5 is requiring security policies. At this point, we feel that there are inconsistencies in the Requirement language as well as potential Compliance Enforcement issues in reference to those particular Requirements. We would ask the drafting team to provide clarity on why Requirement R3 and Requirement R4 mentions Management Plans and Requirement R5 mentions security policies. Additionally, the proposed language in Requirement R3 and Requirement R4 mentions high and medium Impact BES Cyber Systems. Requirement R5 mentions Low Impact BES Cyber Systems. Again, we would ask for clarity on why all three (3) Cyber Systems type aren't included in Requirement R3 through Requirement R5? Finally, we suggest revising Requirement R5 language and moving it to the CIP-003 Standard. In the case that the drafting team doesn't agree with the revising of the Requirement's language, Our group recommends that this Requirement language be moved to the CIP-003 Standard because, we feel that it's the most appropriate Standard to handle this Requirement which is applicable to Low Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	No
Document Name	
Comment	

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

Exelon has the same concerns regarding the lack of a compliance “safety valve”, the potential for double jeopardy as well as the administrative burden of updating the supply chain cyber security risk management plan(s) for newly identified vulnerabilities as included in the comments on R1-R4. The discussion under (4) identifies how the proposed R5 overlaps with existing CIP Standards.

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

We agree with EEI's recommendation to delete R5.

Part 5.2 is duplicative with CIP-003-7, Attachment 1, Sections 2 and 3.

Extending the operational controls for authenticity/integrity in Part 5.1 to low impact BES Cyber Systems is not commensurate with the risk. If the SDT thinks the risk to low impact BES Cyber Systems is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing the massive scope of these low impact systems.

NERC's Compliance Registry Summary of Unique Entities and Functions as of March 3, 2017, identifies 1,398 unique NERC entities. These entities range from entities with a couple breakers for low impact Facilities (lines), to entities operating gigawatts of low impact generation units to entities operating high-impact Control Centers for thousands of miles of medium impact Transmission Facilities, for example. All have BES Cyber Assets, but very different risks.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

- Dominion is of the opinion that all CIP policy requirements should be located in CIP-003 and that all requirements for low impact BES cyber assets should be placed in Attachment 1 of CIP-003. Placing all of the low risk operational CIP requirements in a single standard allows entities that have only low impact cyber assets to reference a single source for pertinent requirements.
- Dominion recommends the following modification to Part 5.1:

5.1: Verify the integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware prior to authorized installation into a low impact BES Cyber System."

- Dominion recommends the removal of Part 5.2. Access control obligations, including system-to-system remote access already exist in Section 3 of Attachments 1 and 2 of CIP-003-7 for low impact. CIP-003-7 is currently pending FERC approval.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

With the applicability of low impact BES Cyber Systems, this appears to negate a comment in CIP-002, R1.3 where it states, "… (a discrete list of low impact BES Cyber Systems is not required)".

What is the timing of R5.1 in terms of new software and existing software? The rationale explains that this starts in the operate/maintain phase of the life cycle but does the timing/life cycle language need to be added to the Standard rather than explained in the rationale section, which may not appear in the final language? Does this apply only to devices in production? For example, what if software is pre-loaded by an OEM. Is there an expectation that the Regional Entities work with their OEM to verify integrity and authenticity prior to this pre-loading? We seek more clarity in the language of R5 and recommend adding "…for Cyber Assets in production."

Regarding the security controls for vendor initiated and system-to-system remote access, R5 is about one or more documented policies and R4 is about the processes for authorization, logging and monitoring, and de-provisioning of remote access. With the requirement of one or more documented cyber security policy, how would Responsible Entities enforce the policy(ies) without also requiring documented plan(s) and process(es), which R5 does not address?

There is no need to have R5 because coverage of low impact BCS is already included in R1. There are two options for R5: integrate it into either (1) existing applicable NERC CIP Standards or (2) R2, R3, and R4 of CIP-013-1.

For option #2:

R2 is about the periodic review and approval of the supply chain cyber security plan(s) developed in R1. R3 obligates Entities to define process(es) to verify the baseline components and any upgrades prior to BCS installation. Requirement R5.1 appears to be identical to R3 because the term "software" in R5.1 is broad in scope and includes the OS and commercially available or open source software.

If Entities are concerned with R4.2 for low impact BCS, the integration of R5 and R4 can either include (1) "per Cyber Asset capability" or "if technically feasible" language for low impact devices or (2) specific language of a risk-based approach, vendor or system, in determining where remote access controls will be applied.

We recommend option #1, the removal of R5 from CIP-013-1 and integration of the requirement into existing applicable NERC CIP Standards.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

R5 discusses a Low policy – NRG recommends that this requirement should be moved to the CIP-003-7i standard where all CIP policy requirements are outlined.

As we reviewed the Requirements applicable to Requirement R3 and Requirement R4, it is to our understanding that a Management Plan needs to be developed and maintained. However, Requirement R5 is requiring security policies. At this point, we feel that this creates inconsistencies in the Standard language as well as potential Compliance Enforcement issues in reference to those particular Requirements (jumping from plans to a policy).

For SDT consideration, there is no access control requirement today for Low Impact Interactive Remote Access which expands the scope broadly to existing CIP standards. This is a similar concern for patching updates (patch management) for Low Impact BCS.

NRG is concerned that in R5.2 the term "controlling" implies operational and technical controls which is inconsistent with a policy level requirement.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1.

If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy.

Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

R5.1 is not consistent with R1.2.5. Recommend changing R5.1 from “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and“ to “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and” As written R5.1 expands the scope or R1.2.5 with little increase to security or reliability

Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing “controlling”

Request that R5 be re-worded to mitigate risk like CIP-003 --- “organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.”

CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request “per system capability” wording for R5. Not all vendors provide a “golden hash” or other mechanism to validate.
- To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.”

9. Does R5 allow the Entity to “accept the risk?”

10. R5.2 should be revised to say, “Ability to disable or otherwise respond to detected unauthorized activity during remote access sessions.”

11. Language of R5 should say “…shall document and implement one or more cyber security policies…” to clarify that implementation is expected for compliance. Draft R5 language does not include the term “implement”.

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	

Same as RoLynda Shumpert's comments from SCE&G:

With the applicability of low impact BES Cyber Systems, this appears to negate a comment in CIP-002, R1.3 where it states, "… (a discrete list of low impact BES Cyber Systems is not required)".

What is the timing of R5.1 in terms of new software and existing software? The rationale explains that this starts in the operate/maintain phase of the life cycle but does the timing/life cycle language need to be added to the Standard rather than explained in the rationale section, which may not appear in the final language? Does this apply only to devices in production? For example, what if software is pre-loaded by an OEM. Is there an expectation that the Regional Entities work with their OEM to verify integrity and authenticity prior to this pre-loading? We seek more clarity in the language of R5 and recommend adding "…for Cyber Assets in production."

Regarding the security controls for vendor initiated and system-to-system remote access, R5 is about one or more documented policies and R4 is about the processes for authorization, logging and monitoring, and de-provisioning of remote access. With the requirement of one or more documented cyber security policy, how would Responsible Entities enforce the policy(ies) without also requiring documented plan(s) and process(es), which R5 does not address?

There is no need to have R5 because coverage of low impact BCS is already included in R1. There are two options for R5: integrate it into either (1) existing applicable NERC CIP Standards or (2) R2, R3, and R4 of CIP-013-1.

For option #2:

R2 is about the periodic review and approval of the supply chain cyber security plan(s) developed in R1. R3 obligates Entities to define process(es) to verify the baseline components and any upgrades prior to BCS installation. Requirement R5.1 appears to be identical to R3 because the term "software" in R5.1 is broad in scope and includes the OS and commercially available or open source software.

If Entities are concerned with R4.2 for low impact BCS, the integration of R5 and R4 can either include (1) "per Cyber Asset capability" or "if technically feasible" language for low impact devices or (2) specific language of a risk-based approach, vendor or system, in determining where remote access controls will be applied.

We recommend option #1, the removal of R5 from CIP-013-1 and integration of the requirement into existing applicable NERC CIP Standards.

Likes 0	
Dislikes 0	
Response	

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	

We propose the SDT modify standard language based on Vectren's proposed language below:

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	

Comment

1) The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1.

2) If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy.

3) Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

4) R5.1 is not consistent with R1.2.5. Recommend changing R5.1 from “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and“ to “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and” As written R5.1 expands the scope or R1.2.5 with little increase to security or reliability

5) Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing “controlling”

6) Request that R5 be re-worded to mitigate risk like CIP-003 --- “organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.”

7) CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

R5 modifies requirements for the Cyber Security Policy, in conflict with CIP-003 R1. It also modifies the approval level required for a Cyber Security Policy (Senior Manager ONLY), allowing a delegate to approve part but not all of a Cyber Security Policy. The entire requirement belongs in CIP-003 and should be reworded to not undermine the governance structure set out in CIP-003 and the authority of the CIP Senior Manager.

CenterPoint Energy recommends that the SDT consider moving the portion of this requirement that is not duplicative to CIP-003 with the rest of the requirements for assets that contain Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	

Comment
OUC is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. OUC requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, OUC requests that all requirements related to low impact assets be included in CIP-003.

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	

Comment
CIP-003-6 R1.2 prescribes policy level controls. CIP-013-1 R5 effectively expands the requirements for policy beyond what is mandated in the current approved and enforceable version of the CIP-003-6 Reliability Standard. Any expansion in scope to CIP-related policy requirements or controls for low impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one. CIP-003-6 R2 requires registered Entities to develop and implement plans for the control of electronic access (which includes remote vendor-initiated user or system-to-system access) thereby rendering CIP-013-1 R5.2 superfluous and unnecessary, as well as placing it at odds with efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value. CIP-003-6 R2 Attachment 1 Section 2 necessitates the implementation of electronic controls for low impact BES Cyber Systems in accordance with the plans developed pursuant to CIP-003-6 R2, thereby further rendering CIP-013-1 R5.2 superfluous and unnecessary, as well as placing it at odds with efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

CIP-002-5 Requirement 1 R1.3 explicitly excludes the requirement for an inventory of low impact BES Cyber Assets through the its parenthetic clause stating, "**a discrete list of low impact BES Cyber Systems is not required**" and CIP-013-1 R5.1 effectively expands this current approved and enforceable requirement through its detailed Cyber Asset-level expectation related to software and firmware and any patches, updates, and upgrades to software and firmware. Any expansion in scope to policy requirements or controls for low impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

Likes 0	
Dislikes 0	

Response

Brian Bartos - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli

Answer	No
Document Name	

Comment

Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE

Answer	No
Document Name	

Comment
1. Supply chain risks may include insertion of counterfeits, unauthorized production, tampering and theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the industrial supply chain. Threats and vulnerabilities created by malicious actors (individuals, organizations, or nation states) are often especially sophisticated and difficult to detect, and thus provide a significant risk to organizations. It is difficult to understand how a low impact entity will be able to detect these risks and protect themselves against code that they have no control over. ACES recommends an approach that allows the vendors a process to communicate with low impact entities on how their product is secure. The vendor should be the focal point not low impact entities who do not have the resources to interact with multiple vendors constantly.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	

Comment
Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016. Reclamation recommends that Requirement R5 be deleted. There would be no need for Requirement R5 if all aspects of the supply chain risk management plan(s) are to be addressed in Requirement R1 and its sub-requirements.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
Rationale for Requirement R5: The rationale language for R5 states, “An entity could apply process(es) used for Requirements R3 and R4 to satisfy its obligations in Requirement R5.” IPC does not see this language reflected in the R5 requirement language. If documented processes are an acceptable means of achieving compliance with R5, IPC suggests rewriting the R5 requirement language to include the terms “processes” or “policies.” Additionally, there is continued creep in the standard language (here and elsewhere) to add requirements for Low Impact BCS, when Responsible Entities are still explicitly not required to have an inventory of Low Impact BCS. If it is the intent of the SDT and regulators to continue adding requirements to Low Impact BCS, IPC recommends a re-

write of CIP-002-5.1 to ensure that all Low Impact BCS are appropriately identified rather than using standards to disagree with current enforceable standard language.

R5

The language of R5, R5.1, and R5.2 state, "Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

"**5.1.** Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and

"**5.2.** Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s)."

IPC does not feel CIP-013-1 is an appropriate standard to address R5, R5.1, and R5.2. IPC believe R5, R5.1 and R5.2 belong in CIP-003-7(i), as R5, R5.1, and R5.2 are related to cyber security policies and low impact BES Cyber System requirements. IPC feels the intent of CIP-013-1 is to address supply chain controls, whereas CIP-003-7(i) addresses cyber security policies (High, Medium and Low) and all low impact BES Cyber System requirements.

IPC feels the requirement to have a policy reviewed by the CIP Senior Manager or delegate is purely administrative and does not provide value and recommends that it should be removed.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. Santee Cooper requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, Santee Cooper suggests that all requirements related to low impact assets be included in CIP-003.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

This requirement should be placed within CIP-003 alongside other requirements applicable to Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA recommends moving R5 to CIP-003 as it applies to Lows only. This will maintain the single standard requirement for entities that only have Low assets. The application of the requirement is not aligned with the current Low Impact BES Cyber System standard CIP-003 that does not require an inventory of equipment and software or identifying system cyber assets. Language and scope should be modified to provide clear scope and compliance requirements.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

1) The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003.

2) R5.1 is not consistent with R1.2.5, should R5.1 include the term “that are intended for use” to read “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and”

3) Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls R5 needs to be a process not a policy. If this is a policy, then suggest removing “controlling”

4) There should be exclusion comparable to a CIP Exceptional Circumstance added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.

5) R5 should be a plan document and not a policy document.

Likes 0	

Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	

Comment
CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	

Comment
Colorado Springs Utilities (CSU) is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CSU requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CSU requests that all requirements related to low impact assets be included in CIP-003.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	

Comment
Seattle City Light is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. Seattle City Light requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, Seattle City Light requests that all requirements related to low impact assets be included in CIP-003.

Likes 0	

Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
It is unclear how the risk and requirements in R5 for Low Impact BES Cyber Systems are differentiated from the other requirements and how the requirements will be measured considering a list of Low Impact systems are not required. There seems to be some reduncancy between R1 and R5 for Low Impact. Suggest removing Low Impact requirements from CIP-013 and incorporating into CIP-003 for consitency.	

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

Why not address this as part of the Cyber Security policy for Low Impact in R1.2 of CIP-003?

Also what about the Cyber Security Policy for Highs and Mediums? Should that also address Supply Chain?

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment

The NYPA Comments

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. SMUD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, SMUD requests that all requirements related to low impact assets be included in CIP-003.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

R1 and R2 are sufficient for addressing vendor risk for LIBCS. Requirements R1 and R2 require Responsible Entities to assess and evaluate ways to mitigate vendor risk. These requirements include LIBCS in addition to MIBCS and HIBCS. We do not believe that extending the operational controls (i.e., authenticity/integrity and remote access) to LIBCS is commensurate with the risk. If the SDT thinks the risk to LIBCS is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing tens of thousands of LIBCS systems. Also, given the complications we raised above regarding compliance with these operational controls for HIBCS and MIBCS, we recommend that the SDT consider deleting R5.

We also note that vendor-based and equipment-based approaches that may be adopted for Requirements R3 and R4 are also likely to further address LIBCS. And part 5.2 is also duplicative with CIP-003-7, Attachment 1, Sections 2 and 3.

We recommend that the SDT consider deleting Requirement R5.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	

Comment

Tacoma concurs with the comments provided by the LPPC.

In addition, it should be noted that CIP-003 R2 requires a plan, while CIP-013 R5 requires a policy. Where LPPC's comments request "that all requirements related to low impact assets be included in CIP-003," this can be accomplished by having the policy language as a portion of CIP-003 R1 part 1.2.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language.	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
This requirement should be placed within CIP-003 alongside other requirements applicable to Low Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

R1 and R2 are sufficient for addressing vendor risk for LIBCS. Requirements R1 and R2 require Responsible Entities to assess and evaluate ways to mitigate vendor risk. These requirements include LIBCS in addition to MIBCS and HIBCS. We do not believe that extending the operational controls (i.e., authenticity/integrity and remote access) to LIBCS is commensurate with the risk. If the SDT thinks the risk to LIBCS is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing tens of thousands of LIBCS systems. Also, given the complications we raised above regarding compliance with these operational controls for HIBCS and MIBCS, we recommend that the SDT consider deleting R5.

We also note that vendor-based and equipment-based approaches that may be adopted for Requirements R3 and R4 are also likely to further address LIBCS. And part 5.2 is also duplicative with CIP-003-7, Attachment 1, Sections 2 and 3.

We recommend that the SDT consider deleting Requirement R5.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

R1 and R2 are sufficient for addressing vendor risk for LIBCS. Requirements R1 and R2 require Responsible Entities to assess and evaluate ways to mitigate vendor risk. These requirements include LIBCS in addition to MIBCS and HIBCS. We do not believe that extending the operational controls (i.e., authenticity/integrity and remote access) to LIBCS is commensurate with the risk. If the SDT thinks the risk to LIBCS is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing tens of thousands of LIBCS systems. Also, given the complications we raised above regarding compliance with these operational controls for HIBCS and MIBCS, we recommend that the SDT consider deleting R5.

We also note that vendor-based and equipment-based approaches that may be adopted for Requirements R3 and R4 are also likely to further address LIBCS. And part 5.2 is also duplicative with CIP-003-7, Attachment 1, Sections 2 and 3.

We recommend that the SDT consider deleting Requirement R5.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

We strongly disagree with requirement R5. The issues with this requirement are too many to list. In particular the SDT should avoid developing mandatory requirements that will reduce the security and reliability of the Bulk Electric System as it has proposed in this instance.

The directive in FERC Order 829 is limited to “the context of addressing supply chain management risks.” According to the definition of supply chain provided in NIST-800-53 (and referenced by FERC in paragraph 32, footnote 61), supply chain ends at the “delivery of products and services to the acquirer.” In the system lifecycle, the supply chain management process occurs prior to the identification of a Cyber Asset as a BES Cyber System pursuant to the implementation of CIP-002-5.1a. This designation must only occur “upon commissioning” for planned system installations (and even later for unplanned changes). Therefore, this BES Cyber System identification, nor its categorization as low impact, does not exist during the supply chain context.

Further, no list of low impact BES Cyber Systems is required. In order to demonstrate compliance with R5, entities would need a list of low impact BES Cyber Systems along with a full system baseline. The net effect of this requirement will be a SIGNIFICANT reduction in security by providing a regulatory disincentive to patch known security vulnerabilities in low impact BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	

Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

The expectations for R5.1 are out of Entity scope for the reasons stated challenging R3. However, Low Impact BCS software and firmware should be expected to be checked for functionality by the Entity.

Likes 0	
Dislikes 0	
Response	

Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No

Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
As this Standard is supposed to be focused on the vendor and as supply chain management risks apply equally to all categorizations of BES Cyber Systems, these requirements are superfluous. Requirement R1 already applies to all BES Cyber Systems and includes these requirement elements. There is no reason to call out requirements specific to Low Impact BES Cyber Systems. If the elements of the plans and processes are vendor-focused as they should be, there is no need to itemize the Low Impact BES Cyber Systems, which is the apparent real reason for Requirement R5 being defined separately.	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No

Document Name	

Comment

1) The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1.

2) If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy.

3) Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

4) R5.1 is not consistent with R1.2.5. Recommend changing R5.1 from “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and“ to “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and” As written R5.1 expands the scope or R1.2.5 with little increase to security or reliability

5) Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing “controlling”

6) Request that R5 be re-worded to mitigate risk like CIP-003 --- “organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.”

7) CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

· Request “per system capability” wording for R5. Not all vendors provide a “golden hash” or other mechanism to validate.

· To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.”

Does R5 allow the Entity to “accept the risk?”

R5.2 should be revised to say, “Ability to disable or otherwise respond to detected unauthorized activity during remote access sessions.”

Language of R5 should say “…shall document and implement one or more cyber security policies…” to clarify that implementation is expected for compliance. Draft R5 language does not include the term “implement”.

Likes 0	
Dislikes 0	

Response

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6

Answer	No
Document Name	

Comment

This requirement implies larger burdens on Low Impact BES Cyber Systems than the upcoming CIP-003-7 changes in regards to patch management and tracking. In neither of the previous versions of CIP-003, was it deemed necessary for patch management controls to be applied to Low Impact BCS. The nonvariable nature of the phrase "…and **any** patches, updates, and upgrades…" states that the Policies implemented to address this requirement will require a validation on every asset with a Low Impact rating. We recommend removing this Requirement and addressing the FERC Directive solely through R1.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5

Answer	No
Document Name	

Comment

See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	No
Document Name	
Comment	
The expectations for R5.1 are out of scope for and Entity for the reasons stated disputing R4. Low Impact BCS software and firmware should be expected to be checked for functionality by the Entity.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes all Low Impact BES Cyber System Controls should go into CIP-003 R1.2, not create a new Requirement under CIP-013.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	

Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 5.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
As currently written, R1 and R5 are applicable to low impact BES Cyber Systems. R5 requires "one or more documented cyber security policies" while R1 requires "one or more documented supply chain risk management plan(s)". CIP-003 requires first a policy and then a plan. Policies are typically higher level documents than plans so consistency is an issue here. R5 is duplicative of the review and approval by CIP Senior Manager required in R2. For consistency with other CIP Standards, CIP-003 R1.1 should be expanded to include supply chain risk management as part of the collective cyber security policies to be reviewed and approved by the CIP Sr. Manager at least every 15 months and removed from CIP-013-1. R5.1 indicates a protection that needs to be applied at the Cyber Asset level, yet R5 is applicable to BES Cyber Systems. This language elevates low impact BES Cyber Systems to the level of medium and high impact BES Cyber Systems. Under existing CIP Standards, Security Patch Management requirements reside in CIP-007 and none are applicable to low impact BES Cyber Systems. Additionally, software and patching typically occurs at the Cyber Asset level and low impact entities are only required to identify assets containing low impact BES Cyber Systems. Implementing R5 applies controls from existing CIP Standards which are not applicable to low impact BES Cyber Systems. It is incongruous to require verification of patches on a low impact BES Cyber System for which there is no requirement to patch. For consistency purposes, this requirement should be placed within the security plan under CIP-003 Attachment 1 for low impact BES Cyber Systems. Current standards have been drafted to allow entities with low impact BES Cyber Systems to have a single place to for security plan requirements.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No

Document Name	
Comment	

- Regarding R5.1, the Standard Drafting Team should clarify what is intended by “[I]ntegrity and authenticity.” This is an ambiguous term which can have different meanings.

- Regarding R5.1, vendor information is proprietary (contractually). Registered Entities should not be held accountable for compliance obligations in which they have no control of.

- Requirements pertaining to BES Low Impact Cyber Systems should be placed within CIP-003 Attachment 1 as originally intended.

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	

As drafted, R5 greatly increases the requirements for low impact BES Cyber Systems and completely ignores the H/M/L impact model. We feel there should be no such requirements for assets deemed to have a low impact on the BES, and that R5 should be struck entirely. If the SDT disagrees, then please clarify how implementation of these requirements would differ for low impact versus a medium or high impact system?

In addition, Tri-State is struggling to see how implementation of this requirement could be accomplished without a maintained inventory of low impact BES Cyber Systems, vendors, and software. This would be an incredibly substantial effort, that we believe the previous V5 drafting team understood well, which is why entities are not required to have a list of low impact BES Cyber Systems. Please clarify how an entity would carry out such policies while keeping with a low risk model.

Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	

Concur with EEI’s Position

Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	
SVP agrees with other entities that requirements imposed on low impact assets be contained in CIP-003.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA recommends that CIP-013-1 R5 be placed within CIP-003 in order to keep consistency with the approach used in the remaining CIP standards. Low impact requirements were placed in CIP-003 in order to keep all requirements within a single standard and requirement. By adding these requirements into a new standard, there is confusion resulting in unnecessary compliance confusion.	
Likes 0	
Dislikes 0	
Response	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.	

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant

Answer	No
Document Name	

Comment

This requirement should be eliminated in its entirety. We have adequate cyber controls in place for low impact Cyber Systems. The classification recognizes that these systems inherently have a low ability to negatively impact the Bulk Electric System. We should focus our resources on those systems that have the potential for significant adverse impact on the BES.

Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

As with other comments, this requirement is duplicative and should be placed within the security plan under CIP-003 Attachment 1 for low impact BES Cyber Systems. Current standards have been drafted to allow entities with low impact BES Cyber Systems to refer to a single standard to for security plan requirements.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company disagrees with the direction the proposed R5 requirement is taking, specifically with regard to the implied requirement to have a system baseline inventory of software and/or firmware on each Low Impact BES Cyber System when such an inventory is explicitly not required by existing CIP Standards. Not only does this create a collision of Standard requirements, but the burden on Responsible Entities would be immense and unmanageable – significantly increasing risk to reliability. Despite interpretation of language in this FERC Order, previous commission Orders have supported not requiring inventories at the Low Impact level. Southern recommends the comments previously provided under R1 to properly scope this Standard to “industrial control system” vendor products and services, within the Supply Chain horizon, where risk to assets containing Low Impact BES Cyber Systems is more appropriately addressed.

If the SDT chooses to keep R5 in the Standard in this manner, Southern provides the below edits to more appropriately scope this requirement towards the ICS vendor products at “assets containing lows.” Again, consideration must be given to modifying this requirement language in a manner that does not introduce an implied responsibility to maintain an inventory of Low Impact BES Cyber Systems, their member Cyber Assets, and/or the individual component software and firmware baselines of those System components.

For example, if an entity has a thousand or more substations, it does not require a device level inventory of all devices in all substations to know the few vendors of relays that would be in those substations. Therefore, the entity would need to document how they deal with the firmware upgrades for those vendors. The same goes for generating plants; the entity does not need to know the thousands of individual devices in a plant to know the DCS or

turbine control vendors per unit. Therefore, having plans and controls for dealing with the software, services, and remote access for those vendors is what is needed.

Additionally, Southern Company disagrees with the placement of this requirement, should it remain in this Standard, recognizing the SDTs time constraints with having to file a new or modified Standard addressing Supply Chain cyber security risks as per the FERC Order. Any requirement addressing controls for assets containing Low Impact BES Cyber Systems should be placed in CIP-003-6 R2, Attachment 1.

Modify R5 language as follows:

R5. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics, based on risk, for its industrial control system vendor products and services at assets containing low impact BES Cyber Systems: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

5.1. Integrity and authenticity of software and firmware and any patches, updates,

and upgrades to software and firmware; and

5.2. Controlling vendor-initiated remote access, including system-to-system remote

access with vendor(s).

Likes 0	
Dislikes 0	

Response

Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
The proposed application of specific requirements to Low Impact BES Cyber Systems in CIP-013-1, R5 appears reasonable.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
While in Agreement with the concept of adding a Requirement for low impact BES Cyber Systems, ACEC does have the following concerns: 1. Part 5.1 requires the Responsible Entity to have one or more cyber security policies for "Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware." This requirement is not consistent with CIP-002-5.1 which states in Requirement 1, Part 1.3 that "a discrete list of low impact BES Cyber Systems is not required." To be able to track security patches and firmware upgrades you will by necessity have to have a discrete list. It is recommended that Part 5.1 be replaced with the Information system planning security controls: this will ensure that security will be part of the planning for low impact Information Systems/Control Systems. 2. Part 5.2 requires the Responsible Entity to have one or more cyber security policies for "Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s)." At present, CIP-003-6 Attachment 1, Section 3 requires only that you (3.1) "For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access;" and "Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability." This new Requirement extends these controls significantly beyond the present CIP-003-6 requirement and should be replaced with the Vendor risk management and procurement security controls: this will ensure that these issues are addressed early in the procurement process and throughout the lifecycle of low impact BES Cyber Systems and their associated Cyber Assets.	

3. This Requirement should be moved to CIP-003-6, where ALL low impact BCS Cyber Systems security controls are addressed. This will allow Registered Entities with only low impact BES Cyber Systems to address only CIP-002-5.1 and CIP-003-6, reducing the potential for confusion. This approach has been taken by SDT 2016-02 in adding Transient Cyber Assets/Removable Media requirements to CIP 003-6 vice including in CIP-010-2 where it is addressed for high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Should a reference to cyber security policies related to this Requirement for Low-impact BCS also be incorporated into CIP-003-7(i) R1.2?	
Likes 0	
Dislikes 0	
Response	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
In the VSL for Requirement R5 there is no recognition of a Responsible Entity that had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, but the approval was more than 18 calendar months. A third entry should be added to the Severe VSL for Requirement that reads: *The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however, the approval was more than 18 calendar months from the previous review.*	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes

Document Name	

Comment

AZPS understands the time constraints associated with the development of this proposed standard, but respectfully asserts that all policy-related obligations should be consolidated into the appropriate requirements of CIP-003. AZPS, therefore, recommends that, upon completion of this standards process, a SAR is entered to consolidate policy-related requirements such as Requirement R5 the existing CIP-003 Requirement R1.2

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

PSEG agrees with the intent of this requirement, but has the following questions/recommendations below:

- Recommend moving CIP-013 R5 to CIP-003 R1.2, to remain consistent with previous decisions to maintain all low impact requirements in CIP-003.

- Request clarification. Requirement R5 requires one or more documented policies. The Rationale for Requirement R5 states “An entity could apply process(es) used for Requirement R3 and R4 to satisfy its obligations in Requirement R5 or could develop a separate policy or processes to address low impact BES Cyber Systems.” Is the intent of R5 similar to R3/R4 that the outcome is “one or more documented processes”? If so, should there be a separate policy requirement added to CIP-003 to have the CIP Senior Manager approve the policy?

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	

Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
As the IESO does not have low impact Bes Cyber Assets we abstain from commenting on this requirement.	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	
Document Name	

Comment	
The IRC and SWG abstains from commenting on this requirement.	
Likes 0	
Dislikes 0	
Response	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Response	

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

In light of the sweeping changes represented by CIP-013, potentially altering the way an entire industry assesses risk, deals with vendors and contractors, and performs security operations tasks, the 1 year after FERC approval effective dates are far too short for implementation.

CenterPoint Energy would like to propose an effective date of at least 24 months following FERC approval. It will be a significant effort for entities to write a plan, negotiate with vendors, train and work with new groups to implement the requirements.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	

Comment

1) R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

2) Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions.

3) Request clarification. The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No
Document Name	

Comment

Entergy seeks clarification on if the implementation date for CIP-013 merely requires that the entity have a CIP supply chain management plan in effect (with the ability to have a rolling implementation of specific protections and controls directed in that plan similar to the CIP-014 implementation), or if all protections and controls directed in the plan (including the potential technical deployment of new devices/systems) must be installed and live on day one of the implementation date. In other words, Entergy notes that the proposed standard recognizes and allows for a multi-phased, or rolling, implementation of the CIP supply chain management plan by not requiring contracts be renegotiated to adopt new terms and conditions; Entergy requests that CIP-013 explicitly allow entities to likewise have a phased or rolling implementation of identified controls and protections measures identified in their security plans after the implementation date.

In the alternative, Entergy cannot support the “12 month” implementation plan and recommends the date be no less than 18 months until more certainty on the extent of technical deployments required by the Standard can be provided. For example, until more clarity is given regarding whether implementation of existing CIP-005 and CIP-007 controls will adequately meet compliance with CIP-013 R4 and R5, or regarding the definition of “vendor remote access.” This is because, depending on the date of passage, the 12 month implementation requirement may fall outside of an entity’s capital planning and budgeting process, resulting in considerable constraints in acquiring funds for significant capital investment to achieve compliance with the standard.

Accordingly, Entergy requests that either a phased or rolling implementation be explicitly approved, or the implementation date be no less than 18 months.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	
Same as RoLynda Shumpert's comments from SCE&G: *With the inclusion of CIP-013 R1 through R5, SCE&G does not agree with the Implementation Plan. We agree with EEI's recommendation of extending the schedule from 12 months to 18 months.*	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems. Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions.	

Request clarification. The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

The implementation Plan refers to “contracts with vendors, suppliers or other entities”; however, Standard refers to only vendors in the text of the Requirements. “Suppliers or other entities” should be removed.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

In the implementation plan for this standard, NRG recommends a staggered implementation plan for R1, R2, & R5 being 15 calendar months. However, NRG recommends a 24-month implementation plan for R3 & R4would be needed for Registered Entities to manage this process on all impacted systems due to the need to re-negotiate processes with vendors (individualized solutions).

The implementation plan should have a timeline for compliance for initial enforcement and subsequent plan revisions – similar to CIP-002 with planned and unplanned changes.

In reference to R1 and contracts, we suggest that the term “future contracts” be addressed in the requirement language such as: “new or modified contracts” on or after the date of Enforcement. These should be vetted in an implementation plan. There will be a conversation of initial compliance versus implemented/ongoing compliance; therefore, NRG requests clear understanding of the implementation plan scope as it pertains to plan reviews, new contracts, modified contracts, and current contracts.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

With the inclusion of CIP-013 R1 through R5, SCE&G does not agree with the Implementation Plan. We agree with EEI’s recommendation of extending the schedule from 12 months to 18 months.

Likes 0	

Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

- Under General Considerations, additional language should be added to address existing contract extensions or addendums, effectively excluding them as well.

For the implementation plan which is 12 months, Dominion recommends an 18 month implementation period for the following reasons:

- Time is needed for entities to assess and impacted contracts relevant to applicable BES Cyber Assets.
- Budgets cycles often extend beyond a 12 month timeframe.
- New environments and assets may be in scope.
- This revision necessitate that entities conduct an impact assessment to determine what changes the revisions create and what is currently in place from the assessments performed for CIP version 6 implementation for low impact BES Cyber System.
- Revision iterations always require some time to assess and verify points of change.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

We do not support the implementation plan based on the proposed changes recommended in approach to addressing the directives. The implementation plan has to be revised to reflect a revised approach.

Implementation of operational cyber security controls changes to standards CIP-002 through -011 should provide for at least two years, especially because of the time it may take some entities if they have to completely revise how their vendors are currently providing service to them.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon generally agrees with the Implementation Plan for CIP-013-1 but offers the following recommendation for clarifying the plan for R2. The initial review and update, as necessary, of cyber security risk management plans specified in Requirement R2 must be completed within fifteen (15) calendar months **following** the effective date of CIP-013-1. There should be no obligation to review the plans ahead of time, and only the initial development and implementation should be required. This should be made clear in the Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes that 12 months from the Effective Date is too short for robust implementation. 18 months might be more appropriate.	
Likes 0	
Dislikes 0	
Response	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	

Resilient Societies recommends a strategic reassessment of how NERC should, in good faith, respond to FERC Order No. 829. Many of the cost-effective remedial initiatives will be beyond the control of the North American electric utilities industry. Fundamental changes in the procurement of IT and OT systems will be required. Also, there are promising cross-industry initiatives to develop Open Source Codes that will better protect industrial control systems and other control systems upon which the electric utility industry depends. NERC should partici;pate in these ongoing initiatives. CIP-01301 imposes too large a burden on roughly 1400 electric utilities within the bulk electric system.

Moreover, the Secretary of Energy has recently-granted (FAST Act) cyber security authority for the broader energy sector. Vulnerabilities of transmission and distribution utilities beyond FERC regulatory authority will foreseeably be channels through which foreign adversaries can attack the bulk electric system includng those portions that are subject to NERC-FERC standards. A broader framework is needed. The current draft Reliability Standard CIP-013-1 imposes substantial costs in time and money, and will not be a cost-effective initiative.

We respectfully urge NERC to provide fresh guidance to the Standard Drafting team to link proposed reliability requirements to broader initiatives, includng the Defense Science Board Report of February 2017 and findings of the Trump Administratioon as it reviews cyber strategy and policy initiatives.This standard will be wasteful of resources, and is not ready for prime time.

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

Seminole Electric comments submitted by Michael Haff

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	No
Document Name	

Comment

R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions.

R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard

Implementation Plan refers to “contracts with vendors, suppliers or other entities”; however, Standard refers to only vendors in the text of the Requirements. “Suppliers or other entities” should be removed.

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1

Answer	No
Document Name	

Comment

Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4

Answer	No
Document Name	

Comment
Based on FE’s comments on the Requirements (R1-R5), review of the Implementation Plan is not relevant at this time.

Likes 0	
Dislikes 0	

Response

John Hagen - Pacific Gas and Electric Company - 3	
Answer	No
Document Name	

Comment
The implementation plan identifies that the effective date will be at least 12 months after the effective date of the applicable governmental authority’s order approving the standard or 12 months after the date the standard is adopted by the NERC Board of Trustees where approval by an applicable governmental authority is not required. Extending the initial review and update, as necessary, of cyber security risk management plans specified in Requirement R2 by as much as 15 months after the effective date of the standard seems to extend the improved supply chain risk management unnecessarily. PGAE believes the initial review and approval of the cyber security risk management plans specified in R2 should be completed on or before the effective date, so that subsequent Requests for Proposal and/or vendor contracts and applicable Service Level Agreements after the effective date can incorporate the R1 controls.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	

Comment
Since the effective date will be at least 12 months after NERC Board of Trustees approval under the current implementation plan, how does extending the initial review and update, as necessary, an additional 15 months provide for improved supply chain risk management? WECC believes the initial review and approval of the cyber security risk management plans specified in R2 should be completed on or before the effective date, so that subsequent Requests for Proposal [RFP] and/or vendor contracts and applicable SLAs after the effective date can incorporate the R1 controls.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SRP does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. SRP requests a 24-month implementation plan.

SRP requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	
Response	

Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	

CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan.

CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

Likes 0	
Dislikes 0	
Response	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	

We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Seminole does not believe that the standard is adequately defined to enable meaningful review of the implementation plan. Further, successful implementation of the plan is highly dependent on vendors and may require more than one year to implement.	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan.

CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan.

CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

Suggest breaking the implementation into three steps which follows CIP-014 – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline

The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities“ however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.” Request clarification.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

AE does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. AE requests a 24-month implementation plan.

AE requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	No
Document Name	

Comment	
PRPA does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. PRPA requests a 24-month implementation plan. PRPA requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan. CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 0	
Dislikes 0	
Response	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	

ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
The implementation plan calls for R2 to be completed 15 months after the effective date of compliance of CIP-013; however, there is no requirement for signing the original R1 plan. Please clarify in R1 or R2 the required signature date for the supply chain cyber security plan.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy proposes an alternative Implementation Plan for the drafting team’s consideration. We agree with an Implementation Plan of 12 months for R1 and R2, and propose an Implementation Plan of 24 months for R3 and R4. We feel that based on the type of work and the workload that will be necessary to comply with R3 and R4 due to these requiring technical controls and configuration changes, a longer implementation plan is required.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Suggest consider phasing the implementation of CIP-013 and CIP-003 Low BCS Physical, Electronic, TCA, and RM to reduce potential for resource constraints created by concurrent implementation of multiple programs.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities, “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.” Request clarification	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 0	
Dislikes 0	
Response	

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
Lack of a NERC definition of a PED makes it uncertain which products this (or any other) CIP standard applies-to. No new CIP standards should be developed until this issue is addressed. One year is not enough time, for the reasons stated above. A minimum of two years should be granted.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item.	
Likes 0	
Dislikes 0	

Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No
Document Name	
Comment	
12 calendar months may be inadequate if contracts are in the negotiation stage. 18 months may be more realistic; however, this is dependent on the language in the final set of requirements. We also recommend that the SDT consider how best to make it clear that this is a forward-looking standard as it relates to contracts, and the associated nuances. For instance, if you have a contract in place that allows for extensions or amendments, do you have to open up the entire contract when extending, making amendments, or minor revisions?	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item	
Likes 0	
Dislikes 0	
Response	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item.	
Likes 0	

Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
Due to the early stage of development of this standard, NRECA is not able to support a specific Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	
SVP agrees with other entities' comments to split the implementation plan into parts, e.g., identify risk, develop a plan and implement a timeline.	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI’s Position	
Likes 0	
Dislikes 0	
Response	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
The Implementation Plan is unfeasible as currently drafted. The proposed Standard should utilize a phased in implementation. In addition, the Standard and Implementation Plan do not address that CIP-013 only addresses new contractual obligations. This lack of clarity will likely cause issues during the enforcement period of the Standard.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
Oxy supports the comments of American Transmission Company, LLC	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Without being able to evaluate the Implementation Plan against the eventual final Standard, the company cannot offer its support.	
Likes 0	
Dislikes 0	
Response	

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
The technical controls required by R3/R4/R5 should be given additional time consideration. Perhaps 24 months to allow time to research and deploy technical controls of R3/R4/R5 while R1 – R2 are policy/contract-language driven only. Would a phased implementation approach be acceptable as a lot of the risks in R3, R4 and R5 have already been mitigated in CIP-007 and CIP-005 and therefore a maturity over time may make more sense?	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	
Comment	
The Standards as currently written require significant modifications to organizational procurement processes for big and small entities alike. Due to the scope of assets being considered, entities must implement central procurement in such a way for every cyber asset to filter through the rigorous process. The number of contracts cutting across BES and non-BES Cyber Systems are too numerous and complex to address as a separate CIP compliance process. This has the potential to require more organizational change than any of the previous version of CIP Cyber Security Standards. In comparison, CIP version 5 implementation allowed for 24 calendar months and fully resourced entities struggled to get the organizational processes	

perfected in time to meet the deadlines. We propose a minimum of 24 calendar months be allowed for the currently drafted Standard. We feel this is appropriate given the minimal time FERC has permitted for this Standard to be submitted.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra

Answer	No
Document Name	

Comment

1) R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

2) Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions.

3) Request clarification. The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

4) Implementation Plan refers to “contracts with vendors, suppliers or other entities”; however, Standard refers to only vendors in the text of the Requirements. “Suppliers or other entities” should be removed.

Likes 0	
Dislikes 0	

Response

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick

Answer	No
Document Name	

Comment

Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

The deferment of R2 by 15 months further supports the idea that the original documents do not have to be approved by the CIP Senior Manager, only subsequent revisions. The Implementation plan should at least require initial approval of the plans that are then subject to periodic review.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC disagrees with the implementation plan. The security controls identified will take significant time to implement, particularly as specified for low impact BES Cyber Systems. The suggestion of a 12 month implementation window implies that fundamentally the SDT does not appreciate the volume and diversity of low impact BES Cyber Systems across North America. Additionally, a 12 month implementation window does not allow time for entities to complete an annual budget cycle. As such, we strongly recommend that the SDT considers an 18 month implementation window at minimum. If any controls are kept for low impact, then a minimum 24 month implementation window should be provided for those controls.

Alternatively, GTC recommends the SDT to work with NERC to immediately begin to take the necessary actions to request more time from FERC to satisfy Order 829. This can be accomplished in 2 phases.

For the first phase, GTC believes the 12 month implementation window can be achieved if the SDT would limit the structure of CIP-013-1 to the supply chain context which ends at the delivery of products/services to the acquirer in accordance with NIST SP 800-53 r4 as outlined in GTC comments number 1 and 3.

For the second phase, GTC encourages for NERC to lay out a plan to FERC to better address the operational/technical requirements of R3 and R4 with the applicable existing CIP standards so that the correct technical experts can develop in a manner that would not create the double jeopardy scenarios described under the comments for R4 and R5. NERC could then request a 24 month window to address the operational technical requirements in the

correct applicable CIP standard. FERC provides NERC discretion per paragraph 44 the option of modifying existing Reliability Standards to satisfy the directive.

GTC recommends the SDT consider GTC's strategy in the comments above, and adapting the Implementation Plan accordingly.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Under initial performance, replace "of" with "following" so that it reads R2 must be completed within fifteen (15) calendar months following the effective date…"

The general considerations section does not explicitly address contract term extensions or other amendments that would not involve renegotiating the contract. We recommend that the SDT add language to address this concern.

We recommend 18 months rather than 12 so that contracts under negotiation can be included. Incorporation of an 18 month implementation plan is also in line with the changes recently approved by industry for the balance of the CIP Standards currently under modification.

We also recommend that the SDT consider adding text to the requirements that make it clear that this is a forward-looking standard. Currently, this forward-looking information only appears in the implementation plan, which may become hidden or lost over time.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No
Document Name	

Comment

The IRC and SWG are unclear how an entity will comply with requirements in R3, R4, and R5 if contracts have not been renegotiated to address the requirements with vendors. Further, clear criteria needs to be identified to determine when an entity must comply with the requirements. The applicability of the Standard should be clarified to address cyber assets procured prior to the CIP-013 effective date. Concerns to be considered include, (1) upon execution of a new agreement with the vendor, (2) upon installation of any new equipment, or (3) upon installation of any new software? Requiring compliance on new equipment or software will be problematic if the contractual agreements do not align.

The IRC and SWG request a 24-month implementation timeframe for CIP-013 R3 and R4 as budget cycle(s) will be required to support contractual issues, implementation, with possible automation of compliance evidence.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Under initial performance, replace “of” with “following” so that it reads R2 must be completed within fifteen (15) calendar months following the effective date…”

The general considerations section does not explicitly address contract term extensions or other amendments that would not involve renegotiating the contract. We recommend that the SDT add language to address this concern.

We recommend 18 months rather than 12 so that contracts under negotiation can be included. Incorporation of an 18 month implementation plan is also in line with the changes recently approved by industry for the balance of the CIP Standards currently under modification.

We also recommend that the SDT consider adding text to the requirements that make it clear that this is a forward-looking standard. Currently, this forward-looking information only appears in the implementation plan, which may become hidden or lost over time.

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment	
LCRA does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. LCRA requests a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

Under initial performance, we recommend replacing “of” with “following” so that it reads R2 must be completed within fifteen (15) calendar months following the effective date…”

The general considerations section does not explicitly address contract term extensions or other amendments that would not involve renegotiating the contract. We recommend that the SDT add language to address this concern.

We recommend 18 months rather than 12 so that contracts under negotiation can be included. Incorporation of an 18 month implementation plan is also in line with the changes recently approved by industry for the balance of the CIP Standards currently under modification.

We also recommend that the SDT consider adding text to the requirements that make it clear that this is a forward-looking standard. Currently, this forward-looking information only appears in the implementation plan, which may become hidden or lost over time.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. SMUD requests a 24-month implementation plan.

SMUD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	
The NYPA Comments	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Implementation plan must clearly state that all these requirements are forward looking and should not impact any existing contracts. We also believe that 12 months may not be enough to fully develop and implement a plan for large organizations to meet all four objectives. Perhaps a 24 month implementation period is appropriate. What is the difference between vendors, suppliers or other entities as stated in the implementation plan in the context of supply chain? None are defined terms.	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	

Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
Seattle City Light does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. Seattle City Light requests a 24-month implementation plan. Seattle City Light requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

The IESO suggest that in order to be consistent with the FERC Order that the standards be forward looking, clear criteria needs to be identified to determine when an entity must comply with the requirements. The applicability of the Standard should be clarified to address cyber assets procured prior to the CIP-013 effective date. Concerns to be considered include, (1) upon execution of a new agreement with the vendor, (2) upon installation of any new equipment, or (3) upon installation of any new software? Requiring compliance on new equipment or software will be problematic if the contractual agreements do not align.

The IESO request a 24-month implementation timeframe for CIP-013 R3 and R4 as budget cycle(s) will be required to support contractual issues, implementation, with possible automation of compliance evidence.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities

Answer	No
Document Name	

Comment

Colorado Springs Utilities (CSU) does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CSU requests a 24-month implementation plan.

CSU requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

Recommendation for a 24-month implementation process.

The implementation for the current CIP-013 standard is short. Many of the systems that are already in place under the current CIP standards were custom created or have features enabled to comply with the requirement(s) which they address. To comply with the standard requirements in CIP-013, in particular R4, registered entities may require modifications to the current processes and systems already in place or may require procurement of new components and/or services. The change process would require coordination with facility/equipment outages. A longer timeframe would be required for entities to effectively manage these changes without a negative impact to BES reliability. Also, to develop a supply chain risk management plan and implement that plan into our contracts would require more than 12 months to implement.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

1) R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

2) Suggest breaking the implementation into three steps which follows CIP-014 – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline

3) The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities“ however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.” Request clarification.

Likes 0	

Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes the lack of clear scope in the standard makes the evaluation of the implementation timeframe ambiguous. If the standard was adopted as written and required Low impact cyber asset inventories identification and evaluation, 24 months would be required to comply with the requirements.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. LCRA requests a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Santee Cooper does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. Santee Cooper requests a 24-month implementation plan.	

Santee Cooper requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

In IPC's opinion, a 12 month effective date is not enough time to implement this standard given the amount of existing CIP standards currently in flux and new standards being developed. In addition, Regulatory guidance is often slow in coming, and entity budgetary cycles are usually at least 12 months. IPC suggests an 18–24 month effective date. An 18-month effective date is also consistent with the CIP-003-7 implementation plan.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation recommends that the implementation schedule be based on risk and enforced using a systematic approach. Under the systematic approach, Reclamation requests that plans affecting high impact BES Cyber Systems would be developed within 12 months of FERC approval, plans affecting medium impact BES Cyber Systems would be developed within 18 months of FERC approval, and plans affecting low impact BES Cyber Systems would be developed within 24 months of FERC approval.

Reclamation recommends that each plan should be implemented within 18 months of being developed.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
It is premature to accept/agree with any implementation plan due to the infancy of this proposed standard and potential risks, impacts, and unintended consequences that may ensue if the CIP-013-1 Standard were to move forward without adequately addressing the concerns of redundancy, lack of clarity, expansion in scope, or contradictory nature of the collective set of proposed requirements as described in above comments. Until the language can be improved so as not to create double jeopardy or an impossibly of non-compliance due to factors outside the control of the Registered Entity, or until a shift in approach can be agreed upon so as to leverage existing enforceable regulations that already provide the intended security or reliability benefit, ATC cannot support the proposed implementation plan.	
Likes 0	
Dislikes 0	
Response	

Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	
OUC does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. OUC requests a 24-month implementation plan. OUC requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
We feel that the approval of the RSAW needs to be included in the documentation. This is another document that is pertinent to the Implementation Plan Process.	
Likes 0	
Dislikes 0	
Response	

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
The proposed 12-month implementation period and specification of an initial performance date for the CIP-013-1, R2 review and update appear reasonable. Texas RE requests the SDT provide a justification for the 12-month implementation period as part of the Standard development process.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	
In conjunction with the comments provided under R1 above, Southern Company supports the SDTs direction proposed in the Implementation Plan where it is applicable to the Supply Chain time horizon and industrial control system vendor products and services used in BES Cyber Systems, but requests the consideration of an 18 month (rather than 12 month) timeframe. For any requirements applicable to assets containing Low Impact BES Cyber Systems, given the volume and complexity of those assets, as well as the volume and diversity of agreements necessary between the Responsible Entity and it's suppliers of ICS products and services, Southern requests the consideration of a 24 month timeframe for implementation.	
Likes 0	
Dislikes 0	
Response	
Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wes Wingen - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
George Tatar - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	
Document Name	

Comment

Twelve months is not sufficient time to allow compliance with all aspects of this standard. The drafting team should consider a phased approach allowing the logical phased implementation of these requirements.

While the Implementation Plan suggests that existing contracts need not be modified, the proposed standard language does not make this clear. ERCOT believes the standard to be a more appropriate location for this exemption, as it is ultimately substantive in nature. ERCOT there recommends that the drafting team include language in the standard explicitly limiting applicability of the requirements to new contracts.	
Likes 0	
Dislikes 0	
Response	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Response	

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

The VLS for R1

- The term "Either of the elements specified" in the Sever VLS is implying two elements when in fact I believe you are meaning "Any of the Elements in Either of the two requirement subparts."
- The High VLS specifies "…did not include one of the elements specified in Parts 1.1 or 1.2". Since one of these elements 1.2.7 is optional by inclusion of the "if applicable" language, this VSL should be rewritten to specifically exclude 1.2.7.

The VSL for R2

- Reviewing and modifying the plan reduce the risk, having a signature does not. Setting arbitrary times frames surrounding missing dates does not reduce risk. Recommend:
  - VSL lower - no signature
  - VSL Moderate - missing a new supply chain security risk during the review
  - VSL High - not performing review within 15 months
  - VSL Sever - not implementing needed control changes as identified from review

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

VSL for Requirement R3

Requirement R3 has four sub-parts which describe the software and firmware which need to be verified. ReliabilityFirst recommends the SDT structure the VSLs similar to Requirement 1 to address each of the sub-parts. ReliabilityFirst offers the following modifications for consideration

Lower VSL – The Responsible Entity implemented one or more documented process(es) for verifying the integrity and authenticity of the software and firmware but did not verify one of the elements specified in Parts 3.1 through 3.4.

Moderate VSL - The Responsible Entity implemented one or more documented process(es) for verifying the integrity and authenticity of the software and firmware but did not verify two of the elements specified in Parts 3.1 through 3.4.

High VLS – The Responsible Entity implemented one or more documented process(es) for verifying the integrity and authenticity of the software and firmware but did not verify three of the elements specified in Parts 3.1 through 3.4.

Severe VSL - The Responsible Entity did not implement one or more documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement.

VSL for Requirement R5

To account for instances where the Responsible Entity had cyber security policies specified in the requirement but were not reviewed for 18 months or greater, ReliabilityFirst recommends the following “OR” statement be added to the Severe VSL Category:

Additional Severe VLS - The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 18 calendar months from the previous review.

Likes 0

Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	
Response	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI does not agree with the requirements as written and accordingly cannot agree with the proposed VRFs and VSLs proposed for those requirements in CIP-013-1.	
Likes 0	
Dislikes 0	
Response	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	

CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	
Response	

Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	

PRPA does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, PRPA requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. PRPA requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Response	

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	
AE does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, AE requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late. For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. AE requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	

For R3 and R4: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted.

Do not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Suggests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	No
Document Name	

Comment

CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

W. Dwayne Preston - Austin Energy - 3

Answer	No
Document Name	

Comment

I support the comments of Andrew Gallo at Austin Energy.

Likes 0	
Dislikes 0	

Response

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

Seminole does not believe that the standard is adequately defined to enable meaningful review of the VRF and VSL.

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Response	

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	
Comment	
CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late. For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 0	
Dislikes 0	
Response	

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	
SRP does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, SRP requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.	

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. SRP requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

WECC believes missing one of the elements of Part 1.2 in the VSL for Requirement R1 should be considered lower risk than missing one of the elements in Part 1.1, as it seems to be a subset of Part 1.1., and should be assessed at moderate risk. WECC agrees that missing one of the elements of Part 1.1 is appropriately identified as a High VSL.

In the VSL for Requirement R5 there is no language for a Responsible Entity that had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, but the approval was more than 18 calendar months from the previous review. WECC believes a third entry should be added to the Severe VSL for Requirement that reads:

The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however, the approval was more than 18 calendar months from the previous review.

Additionally, in the high and severe VSL language of R5 it appears that the word "but" before the words "did not include" should be deleted.

Likes 0	
Dislikes 0	

Response

John Hagen - Pacific Gas and Electric Company - 3

Answer	No
Document Name	

Comment

PGAE believes missing one of the elements of Part 1.2 in the VSL for Requirement R1 should be considered lower risk than missing one of the elements in Part 1.1, as it seems to be a subset of Part 1.1., and should be assessed at moderate risk. We agree that missing one of the elements of Part 1.1 is appropriately identified as a High VSL.

Likes 0	

Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	
Based on FE’s comments on the Requirements (R1-R5), review of the VRFs and VSLs is not relevant at this time.	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Response	

William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
We have not reviewed with care, but consider the standard requirements need fundamental reworking before addressing VRFs and VSLs.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
There is a concern that there is an inconsistency with the risk impact classification for the Requirements, and VSLs. We feel that these inconsistencies have the potential to lead to Compliance Enforcement issues in reference to the proper alignment of both sections. For example, the VSLs for Requirement R3 and Requirement R4 focus on high and medium, however, Requirement R5 mentions low impact. We feel that all three (3) classifications need to be considered in all of the Requirements language to have a successful Standard.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	
Comment	
The VRFs and VSLs will need to be incorporated in CIP-002 through -011 where changes are made.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	

Comment

- We recommend that requirements R1 and R2 should be low based on the fact the requirements are administrative in nature (i.e., deal with the procurement), and if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
- We recommend that requirement R5 should be Low because it is related to CIP-003-6 which is also Low.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	

Comment

Due to our concerns expressed in this document, we did not find it useful to review the VRFs and VSLs at this time.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	

Comment

There is a concern that there is an inconsistency with what is stated in the Requirements, VRFs, and VSLs. These inconsistencies have the potential to lead to Compliance Enforcement issues in reference to those particular elements of the Standard and therefore, NRG recommends alignment between

Requirements, VRFs, and VSLs. NRG suggests that this language be properly aligned with the requirements (recommendation for Low or Moderate VSLs relating to process controls) or else this could lead to future Compliance Enforcement issues for the industry.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted.

For R4: See comment above for R3.

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5

Answer	No
Document Name	

Comment

Same as RoLynda Shumpert's comments from SCE&G:

Due to our concerns expressed in this document, we did not find it useful to review the VRFs and VSLs at this time.

Likes 0	

Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	
Comment	
1) For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL. 2) For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted. 3) For R4: See comment above for R3.	
Likes 0	
Dislikes 0	

Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The VRFs and VSLs seem harsh. CenterPoint Energy does not agree with the automatic High VSL for any element not fully addressed, in a Regional Entity's opinion, by a Responsible Entity's risk management plan, especially given the extremely vague bounds presented on what represents a valid risk management methodology, planning process, evaluation method, or mitigation effectiveness measure.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Response	
Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	
OUCX does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, OUC requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late. For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. OUC requests considering all of the nine sub-requirements of	

R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
It is premature to accept/agree with the VRFs or VSLs due to the infancy of this proposed standard and potential risks, impacts, and unintended consequences that may ensue if the CIP-013-1 Standard were to move forward without adequately addressing the concerns of redundancy, lack of clarity, expansion in scope, or contradictory nature of the collective set of proposed requirements as described in above comments. Until the language can be improved so as not to create double jeopardy or an impossibly of non-compliance due to factors outside the control of the Registered Entity, or until a shift in approach can be agreed upon so as to leverage existing enforceable regulations that already provide the intended security or reliability benefit, ATC cannot support the proposed VSLs/VRFs.	
Likes 0	
Dislikes 0	
Response	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	

Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
The sub-requirements within each requirement should be used to distinguish the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs).	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
IPC feels all VSLs should be set to low the first year of enforcement and then increase the VSL after year one of enforcement. This allows for process refinement without significant penalty.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Santee Cooper does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Santee Cooper suggests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Santee Cooper suggests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and constructs the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. LCRA requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA suggests the VRFs and VSLs include consideration for instances where the vendor or supplier is not able or is unwilling to support the standard requirement.

Likes 0	

Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	

Comment
1) For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL. 2) For R3 and R4: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted. 3) Do not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Suggests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

Likes 0	
Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	

Comment
CPS Energy supports the comments provided by APPA

Likes 0	
Dislikes 0	

Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	

Colorado Springs Utilities (CSU) does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CSU requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CSU requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

The IESO requests review to ensure violations align with impact ratings and existing standards program.

For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, policies and plans are implemented while processes are performed. If a policy or plan is required to be implemented and there is an instance where a process included as part of the policy or plan, is not adhered to, then this would result in a violation of the policy or plan but not in the requirement to implement the policy or plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not

followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted

For R4: See comment above for R3.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

Seattle City Light does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Seattle City Light requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Seattle City Light requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

Linda Jacobson-Quinn - City of Farmington - 3

Answer	No
Document Name	

Comment

FEUS supports the comments submitted by APPA

Likes 0	
Dislikes 0	

Response
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment
FMPA agrees with comments submitted by American Public Power Association.

Likes 0	
Dislikes 0	

Response
Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment
The NYPA Comments

Likes 0	
Dislikes 0	

Response
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, SMUD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. SMUD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Due to our concerns expressed above, we did not find it useful to review the VRFs and VSLs at this time.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	

Comment

Tacoma concurs with the comments provided by the LPPC.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC

Answer	No
Document Name	

Comment

SDG&E agrees with EEI comments and proposed language.

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. LCRA requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Due to our concerns expressed above, we did not find it useful to review the VRFs and VSLs at this time.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No
Document Name	

Comment

The IRC and SWG requests review to ensure violations align with impact ratings and existing standards program.

For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, policies and plans are implemented while processes are performed. If a policy or plan is required to be implemented and there is an instance where a process included as part of the policy or plan, is not adhered to, then this would result in a violation of the policy or plan but not in the requirement to implement the policy or plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted

For R4: See comment above for R3.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Due to our concerns expressed above, we did not find it useful to review the VRFs and VSLs at this time.

Likes 0	

Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC recommends the SDT consider GTC's comments above, and adapting the VRFs and VSLs accordingly.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The VRF mapping based on the ERO Final Blackout Report is questionable because CIP-013 only addresses the possible inclusion of non-authentic or compromised hardware, firmware, and software; and does not speak to the risk level of the inclusion. The same compromised hardware, software, or firmware will pose different risks to the BES based upon the inherent risk to the BES by the Entity. The VSL's are acceptable from a documentation administration standpoint, but do not correspondinly map to the impact resulting. While it is now appropriate to be generating ideas on VRF and VSL for CIP-013, a final determination should wait until the industry is closer to consensus on the actual requirements.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	

Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	

Comment
Requirement R2 calls for the periodic review of existing plans and approval of updates. This is mostly a documentation management requirement and the VRF could be defined as Lower instead of Medium. Compromised software integrity is a key element of previous successful cyberattacks, including Havex. The VRF for Requirement R5 needs to be Medium even though the focus of the Requirement is on Low Impact BES Cyber Systems. The Severe VSL for Requirement R1 should refer to failing to include two or more elements of Parts 1.1 or R1.2. While that should be able to be presumed from the lesser applicability of the High VSL for R1, it is not sufficiently clear.

Likes 0	
Dislikes 0	

Response

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	

Comment
Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	

Comment
1) For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements

of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

2) For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted.

3) For R4: See comment above for R3.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5

Answer	No
Document Name	

Comment

See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

The VRF mapping based on the Final Blackout Report is questionable because CIP-013 only addresses the possible inclusion of non-authentic or compromised hardware, firmware, and software; and does not speak to the risk level of the inclusion. The same compromised hardware, software, or firmware will pose different risks to the BES based upon the inherent risk to the BES by the Entity. The VSL's are acceptable from a documentation

administrative standpoint, but do not map to the risk presented. While appropriate to be generating ideas on VRF and VSL, final determination should wait until the industry is closer to consensus on the actual requirements.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Without being able to evaluate the VRFs and VSLs against the eventual final Standard, the company cannot offer its support.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	

Oxy does not agree with the proposed language of the requirements and therefore cannot agree with the VRF's and VSL's until requirements are revised and updated and corresponding updates are made to the VRF's and VSL's.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Concur with EEI's Position

Likes 0	
Dislikes 0	

Response

Val Ridad - Silicon Valley Power - 1 - WECC

Answer	No
Document Name	

Comment

-- See comments from APPA, with which SVP agrees.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

Due to the early stage of development of this standard, NRECA is not able to support a specific set of VRFs and VSLs.

Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

For R5, the mention of part 5.1 should be removed for High and Critical (see comments on R5 above).

Likes 0	
Dislikes 0	

Response

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

No Comments

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

We agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), provided that they should be updated to reflect changes to the proposed Standards Requirements consistent with the recommendations discussed in questions 1-6.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

In light of all previous comments made above, Southern Company requests that the SDT also consider the VSLs for R3, which should accommodate other levels of severity with regard to verifying integrity and authenticity of industrial control system vendor products, software, patches, and/or upgrades. As currently written, any violation of R3 is considered Severe. There are more granular levels of severity to be considered, for example – when a Responsible Entity has a plan(s), has implemented that plan(s), but a percentage of a volume of patches applicable to a particular business unit (out of many business units within a Responsible Entity) were not adequately validated.

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF

Answer	
Document Name	

Comment

N/A

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response
Kenya Streeter - Edison International - Southern California Edison Company - 6
Answer	
Document Name	
Comment
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison
Likes 0	
Dislikes 0	
Response
Fred Frederick - Southern Indiana Gas and Electric Co. - 3
Answer	
Document Name	
Comment
No comment
Likes 0	
Dislikes 0	
Response
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1
Answer	
Document Name	
Comment
Vectren does not vote in non-binding polls. (VRFs and VSLs).
Likes 0	
Dislikes 0	
Response

Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	
Document Name	
Comment	
These will be reviewed in-depth after changes are made to the requirements.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Response	

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Response	

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The Technical Guidance and Examples makes it more evident as to how much of CIP-013 is duplicative of exisiting CIP Standards. CenterPoint Energy strongly recommends that the CIP-013 draft be edited as noted and the Technical Guidance and Examples be revised accordingly.	
Likes 0	
Dislikes 0	
Response	

Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	
Comment	
1) The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”.	

2) The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

3) The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

4) Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

5) Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

6) Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

7) Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

8) Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

9) Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

10) Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

11) Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

12) Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

13) Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

1) Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

2) Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

3) Page 6., line 5. Notification of all “identified, threatened attempt” is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor’s security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

4) Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition.

5) Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”.

6) Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”.

7) Page 11, Line 15, replace supplier with Vendor.

8) Page 11, line 25, replace “should” with “may”

9) Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

10) Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

11) Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

12) Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

13) Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.

R1

R1.2.2 -- • Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle.

1.2.4 – same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor?

1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates.

1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities.

R2

Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader.

R3

How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit?

Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors.

Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above.

R4

Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	

Same as RoLynda Shumpert's comments from SCE&G:

Although the Guidelines and Technical Basis document has been helpful, it will need further changes to reflect the changes in the requirements driven by concerns of Regional Entities.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”.

The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

Page 6., line 5. Notification of all “identified, threatened attempt” is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor’s security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition.

Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”.

Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”.

Page 11, Line 15, replace supplier with Vendor.

Page 11, line 25, replace “should” with “may”

Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

Page 16 line 25, replace “should” with “may”.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Although the Guidelines and Technical Basis document has been helpful, it will need further changes to reflect the changes in the requirements driven by concerns of Regional Entities.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	

- Recommend removing the responsible entities section in this document as the entities are already outlined in the Standard itself.
- Page 1 Line 42: additional language should be added to address existing contract extensions or addendums, effectively excluding them as well.
- Recommend revising this document based on the revisions made to CIP-013.

Likes 0	
Dislikes 0	
Response	

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No
Document Name	
Comment	

Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.

R1

R1.2.2 -- • Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle.

1.2.4 – same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor?

1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates.

1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities.

R2

Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader.

R3

How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit?

Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors.

Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above.

R4

Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

CIP-002 through -011 Guidelines and Technical Basis should be updated to reflect revisions to those standards and to ensure there is not conflicting guidance.

Outside of the Guidelines and Technical Basis in the standards, other implementation guidance could be proposed for the ERO deference process.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.

R1

R1.2.2 – Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle.

1.2.4 – Same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor?

1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates.

1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities.

R2

Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader.

R3

How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit?

Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors.

Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above.

R4

Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Response

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins

Answer	No
Document Name	

Comment

Technical Guidance and Examples

Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.

R1

R1.2.2 -- • Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle.

1.2.4 – same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor?

1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates.

1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities.

R2

Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader.

R3

How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit?

Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors.

Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above.

R4

Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

We feel that there is inconsistency with the language of the Requirements and The Technical Guidance language specifically in reference to Requirement R3 and Requirement R4. The guidance section for both Requirements mentions reviewing security policies. However, the Requirements mention Risk Management Plans. We feel that this language needs to be properly aligned or this will lead to future Compliance Enforcement issues for the industry.

Likes 0	
Dislikes 0	

Response

OSI Open Systems International - OSI Open Systems International - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

As a vendor of SCADA/EMS/TMS systems for many NERC Responsible Entities, OSI (Open Systems International Inc.) is providing the following comments to the NERC CIP-013 SDT for consideration. All suggested text additions are identified in ***bold-italics*** font.

R1.1.1 Identify and assess risk(s) during the procurement and deployment of vendor products and services;

OSI recommends that the SDT consider an additional comment for paragraph 5 as follows:

Personnel background and screening practices by vendors. ***Note that state & local laws may prevent vendors from sharing certain private information about their employees as related to their background screening (eg. social security numbers).***

OSI recommends that the SDT consider an additional comment for paragraph 9 as follows:

System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout their processes. ***Vendor policies showing adherence to appropriate industry standards for secure development processes is an acceptable method for Responsible Entities to demonstrate due diligence. An example of acceptable industry standards for secure development are the various System & Services Acquisition (SA) controls related to SDLC within NIST 800-161.***

Note that NIST 800-161 is the standard used by U.S. Government entities to ensure Supply Chain Security for all departments and sites.

OSI recommends that the SDT consider an additional comment for paragraph 10 as follows:

Review of certifications and their alignment with recognized industry and regulatory controls. ***It is important that Responsible Entities consider which industry certifications are applicable for each vendor's line of business and not use a "one size fits all" approach. For example, NIST 800-161, ISO-27001 are relevant standards pertaining to computer system security. On the other hand, inclusion of requirements for non-relevant or specialized certifications could disqualify certain vendors (eg. certifications used by the financial industry).***

R1.2 Potential Procurement Controls

It is OSI's opinion that the current CIP-013 non-prescriptive approach to the development of procurement controls will lead to an unsustainable permutation of controls and associated contracts for vendors supporting the industry. The extreme diversity of procurement controls/contracts may push certain vendors away from the bidding process, ultimately reducing competition and increasing costs for the industry as a whole. OSI strongly urges that NERC and the CIP-013 SDT consider the addition of acceptable examples of compliance for different classifications of industry vendors eg. SCADA software vendors, RTU vendors, transformer vendors, etc. NERC and Regional Entity endorsement of such examples will provide both vendors and entities with a sensible baseline for procurement controls. OSI is providing an example of guidance for SCADA/EMS vendors as follows:

The following represents example procurement controls that can be considered for EMS/TMS/SCADA system vendors. This set of controls is not the only method of achieving compliance, but it is considered by NERC to be one acceptable method.

The following "National Institute of Standards and Technology" (NIST) standards can be used to satisfy R1.2. Controls that are applicable to the EMS/TMS/SCADA vendor should be extracted from the various sections to utilize within a procurement contract for compliance with R1.2.

- ***NIST 800-161: "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"***
- ***AC – Access Controls***

- ***AT – Security Awareness and Training***
- ***AU – Audit and Accountability***
- ***CA - Security Assessment and Authorization***
- ***CM – Configuration Management***
- ***CP – Contingency Planning***
- ***IA – Identification and Authentication***
- ***IR – Incident Response***
- ***MP – Media Protection***
- ***PE – Physical and Environmental Protection***
- ***PL – Security Planning***
- ***PM – Security Program Management***
- ***PS – Personnel Security***
- ***PV – Provenance***
- ***RA – Risk Assessment***
- ***SA – System and Services Acquisition***
- ***SC – System and Communications Protection***
- ***SI - System and Information Integrity***
- ***NIST 800-82 "Guide to Industrial Control Systems (ICS) Security***

R1.2.3 Processes for disclosure of known vulnerabilities:

The guidance document currently states the following: "*Request vendor cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed."*

Vendor release of information concerning **uncorrected** non-public vulnerabilities represents a security threat for the entire industry and is contrary to best practices in the software industry and most vendor's security policies. When a vendor provides such information to a single Responsible Entity, the entire industry is placed at further risk of the information being publically released without a mitigation. There are many industry documents on this topic and as an example OSI strongly urges that SDT review the "Vulnerability Disclosure Framework" documented on the DHS website from the National Infrastructure Advisory Council at the following link:

https://www.dhs.gov/sites/default/files/publications/niac-vulnerability-framework-final-report-01-13-04-508.pdf

The DHS publication states the following as part of its overall recommendations to the President:

"Protect the confidentiality of vulnerabilities for which no known exploitations have been reported while affected vendors are working towards a solution. Coordinate the voluntary disclosure of information regarding exploited vulnerabilities to take into account, among other factors, the risks of damage to the nation's critical infrastructure, the need for completion of ongoing investigations, and the coordinated release of solutions or remedies for the vulnerability."

Some Responsible Entities may believe that they can protect such critical information, but the reality is that their protection is only as strong as their weakest employee clicking on a phishing link. When you consider releasing uncorrected or unmitigated vulnerability details to multiple Responsible Entities of all sizes and levels of security training, the risk of that information falling into the hands of bad actors becomes very high.

OSI therefore strongly urges NERC and the CIP-013 SDT to remove the word "**uncorrected**" from the guidance statement. OSI believes it is critically important to utilize language that does not attempt to compel or otherwise recommend that Responsible Entities request disclosure of uncorrected or unmitigated vulnerabilities from any vendor. OSI will not agree to provide such information and most other vendors will likely adopt the same position. On the other hand, vendors that do agree to these provisions and the entities receiving such information are placing the entire industry at further risk until a mitigation is made available by the vendor – which could be weeks or months after bad actors become aware of the vulnerability. Responsible vendors will not disclose uncorrected vulnerabilities but will provide recommended mitigations if they are available.

R1.2.5 Processes for verifying software integrity and authenticity of all software and patches that are intended for use:

OSI recommends additional wording in the final paragraph as follows:

When third-party components are provided by the vendor, request vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses ***within a reasonable period that enables the vendor to integrate and complete certification testing of the updated third-party component.***

R1.2.6 Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and

OSI recommends additional wording in the 3rd paragraph as follows:

Request vendors maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity. ***The vendor's use of a proxy or intermediate host to provide isolation of connections to Responsible Entity's equipment is one example of best practices for remote access.***

R1.2.7 Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable

OSI recommends additional wording in the 1st paragraph as follows:

Request vendors provide Responsible Entity with audit rights that allow the Responsible Entity or designee to audit vendor's security controls, development and manufacturing controls, access to certifications and audit reports, and other relevant information. ***Responsible Entity review of vendor audit reports completed by industry recognized certification groups can be used as an acceptable method to verify a vendor's security posture. Examples are certified auditor reports for ISO-27001, NIST, etc.***

R4 Part 4.1 Potential Remote Access Controls

Based on the NERC Lessons Learned document at this link (http://www.nerc.com/pa/CI/tpv5impmntnstdy/Vendor%20Access%20Management%20Lesson%20Learned.pdf) , OSI recommends additional wording as follows:

One acceptable example of best practice is to use a process whereby the remote access session is initiated by the Responsible Entity, and the token code is provided verbally from the Entity to the vendor when requested by the authentication system. This method ensures that the Responsible Entity is in control of the session and the vendor is not allowed access without knowledge of the Entity.

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	
Comment	

The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”.

The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan.

Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple places in this document.

Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

Page 6., line 5. Notification of all “identified, threatened attempt” is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor’s security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition.

Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”.

Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”.

Page 11, Line 15, replace supplier with Vendor.

Page 11, line 25, replace “should” with “may”

Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

Page 16 line 25, replace “should” with “may”.

The Implementation Plan should more clearly state that contract renegotiation is not necessary during the implementation period if a contract has already begun.

“Vendor” should be a defined term. The Standard should have consistent use of the terms, i.e., only use “vendor” and do not say “third-party.”

Are sub-component manufacturers included under the term “vendor”?

Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	No
Document Name	
Comment	
Too many changes to the standard to adequately comment on the *Technical Guidance and Examples* document.	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	
Based on FE's comments on the Requirements (R1-R5), a detailed review of the Technical Guidance and Examples document is not relevant at this time. However, FE suggests that, in general, it would be helpful if the Technical Guidance and Examples document could provide evidence formats, similar to what is provided in CIP-003-6 Attachment 2.	
Likes 0	

Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

SRP requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

SRP requests clarification on the term “supplier” as it is used in the guidance document. SRP requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, SRP requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. SRP requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced SRP requests that the SDT define the term and place it in the NERC Glossary of Terms.

SRP requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. SRP requests that the following language be added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, SRP requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	

Comment

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	

Comment

We agree with the LPPC/APPA comments.

Likes 0	
Dislikes 0	

Response

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	
Comment	

Portions of the *Technical Guidance and Examples* document that may affect how the standard is interpreted for audit purposes should be placed in the standard's Guidelines and Technical Basis section and needs to be balloted and approved by industry. As this is not a part of the standard and is not a CMEP Practices Guide, this document should provide implementation guidance in a manner consistent with the NERC Compliance Guidance Policy "to develop examples or approaches to illustrate how registered entities could comply with a standard that are vetted by industry and endorsed by the ERO Enterprise." The implementation guidance is an important item for this standard and Seminole appreciates this work.

As implementation guidance, this document should provide a clear standard manner to address requirements for R1.1 and R1.2.1-R1.2.6, while entities may be able to ask additional questions. While the document discusses ideas of what to include, the biggest value would be to provide an example set of specific questions to vendors on risk management controls. By setting this specification up front, costs drop for both vendors and entities as the vendors can provide the basic set of information in a defined format. Once vendors have a better defined set of expectations, they then know how to meet these expectations across the industry, Further, vendors focused on the electric sector will provide this information, as we are their market. However, we all also use smaller software and hardware vendors that primarily service a broader market, and these smaller vendors would be less willing to provide custom information for separate electric sector entities for a sale amounting to tens or hundreds of dollars.

Open source software does not have a cost or a defined vendor. Risk assessment of open source software should be specifically addressed.

As there is no consistency in the software industry on use of hash functions, guidelines need to be provided on what is considered an acceptable approach to meet this requirement.

This standard essentially eliminates the ability to purchase equipment or services on an emergency basis without a pre-existing contract. This will interfere with incident response and BES recovery operations under extraordinary circumstances.

Likes 0	
Dislikes 0	
Response	

W. Dwayne Preston - Austin Energy - 3

Answer	No
Document Name	
Comment	

I support the comments of Andrew Gallo at Austin Energy.

Likes 0	
Dislikes 0	
Response	

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	No
Document Name	

Comment

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

AE requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

AE requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

AE requests clarification on the term “supplier” as it is used in the guidance document. AE requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, AE requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. AE requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced AE requests that the SDT define the term and place it in the NERC Glossary of Terms.

AE requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. AE requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, AE requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	No
Document Name	

Comment

PRPA requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

PRPA requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

PRPA requests clarification on the term “supplier” as it is used in the guidance document. PRPA requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, PRPA requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. PRPA requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced PRPA requests that the SDT define the term and place it in the NERC Glossary of Terms.

PRPA requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. PRPA requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, PRPA requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3

Answer	No
Document Name	

Comment

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5

Answer	No

Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
As the SDT addresses the comments above regarding the standards, we assume the Technical Guidance and Examples will be modified accordingly.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The Guidelines and Technical Basis should include examples to illustrate how implementation is envisioned, and how entities are to be expected to coordinate between SME's and procurement organization, which up to now has not been engaged directly in NERC CIP implementation.	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	No
Document Name	
Comment	

More focus should be given to implementation as opposed to justification. I think we all agree with respect to the importance of making sure the Supply Chain is free of malware and although some justification may be necessary to further explain the merits of adding a few additional requirements to the process, overall we are more concerned with implementation strategy. Those implementation methods would better serve us in our own internal controls and for evidence preparation in order to meet the compliance objectives.

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott; Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen
Dislikes 0	

Response

Thomas Foltz - AEP - 5

Answer	No
Document Name	

Comment

AEP is concerned about the use of the term “should” in the *Technical Guidance and Examples* document. While AEP understands that the intent of this document is to provide guidance and examples, the use of term “should” may be interpreted by the regional auditors as closer to a mandatory requirement. In order to address this concern, the document could use the term “may” instead. AEP is concerned that this is a shift away from traditional guidelines and technical basis documents, which documents the drafting team’s considerations. The proscriptive nature of this document is concerning when left to the interpretation of different auditors. AEP would not want this document to become akin to an actual Requirement without going through the proper process.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See APPA's, TAP's, and USI's comments.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	

The statement on p.1 that CIP-013-1, “does not require the Responsible Entity to renegotiate or abrogate existing contracts,” implies that no action needs to be taken for existing PEDs. This point should be made explicit in the standard per se, but our “additional comments” concerns would still apply for replacing or upgrading existing equipment.

The Technical Guidance and Examples document should be revised to address our negative-ballot comments. Our concerns regarding willingness and ability of vendors to be CIP-013-friendly appear to already be at least partly recognized, ref. for example the statement on p.3, “Obtaining the desired specific cyber security controls in the negotiated contract may not be feasible with each vendor.” The subsequent comment that “every negotiated contract will be different,” indicates however that we and the SDT are not on common ground regarding practicality.

Likes 0	
Dislikes 0	
Response	

faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	

The standard as written doesn’t clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	
Response	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

Although NERC’s Compliance Guidance Policy document describes certain procedures by which a drafting team may provide Compliance Guidance, ERCOT suggests that it is generally preferable to provide examples of acceptable conduct in the standard itself, rather than in an ancillary document, which Responsible Entities would have to remember and separately locate and review. The team could achieve this purpose by using language in the standard such as: “Practices that comply with this requirement include, without limitation, the following: . . . .” ERCOT notes that in a number of

instances, the draft Technical Guidance and Examples document uses normative language (e.g., “should”), rather than permissive (e.g., “may”) language, which suggests that the Technical Guidance document is instead intended to serve simply as a more detailed set of requirements, as opposed to describing one of potentially many acceptable methods of achieving compliance. For example, the guidance for R1 states: “In implementing Requirement R1, the responsible entity should consider the following: . . . .” To the extent the drafting team intends the guidance in this document to be followed, it should be included in the standard.

Likes 0	
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot on this item.

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot on this item.

Likes 0	
Dislikes 0	

Response

Luis Rodriguez - El Paso Electric Company - 6

Answer	No
Document Name	

Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot on this item.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
Due to the early stage of development of this standard, NRECA is not able to support specific Technical Guidance and Examples.	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI's Position	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	

Oxy does not agree with the proposed language of the requirements and therefore cannot agree with the *Technical Guidance and Examples* document until requirements are revised and updated and corresponding updates are made to the *Technical Guidance and Examples* document.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	No
Document Name	

Comment

Without being able to evaluate the Technical Guidance and Examples document against the eventual final Standard, the company cannot offer its support.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

We generally agree with EEI’s comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	No
Document Name	

Comment
The Technical Guidance Document is well-written based upon what the NERC Drafting Team had to work with, but the controls recommendations are expansive enough to become its own industry. This would be an excellent document to use as a starting point of conversation with our hardware and software supply chain, but to impose it on the Entities as the end customers of these ICS products and applications would be overly burdensome with very little return on investment. This would be particularly true for those Entities dealing only with Low Impact BCS.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	

Comment
See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	

Comment
1) The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”. 2) The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two. 3) The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

4) Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

5) Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

6) Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

7) Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

8) Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

9) Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

10) Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

11) Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

12) Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

13) Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

14) Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service

acquisition and implementation". It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting "and/or operational phase of".

15) Page 6, line 1. Provide explanation on how the term "vendor" used in the requirements relates to "supplier's system component, system integrators, or external service providers."

16) Page 6., line 5. Notification of all "identified, threatened attempt" is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor's security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

17) Page 6, line 6: Is the ("Security Event") being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that "have potential adverse impacts to the availability or reliability of BES Cyber Systems" be part of the definition.

18) Page 6, line 22: For R1.2.2: The requirement for the "process for notification" is very different than the "request vendor cooperation" guidance given. Request clarification as to how this guidance for "requested cooperation" would meet the required "notification".

19) Page 9 lines 6 and 8: correct numbers "2.2" and "2.3" to be "2.1" and "2.2".

20) Page 11, Line 15, replace supplier with Vendor.

21) Page 11, line 25, replace "should" with "may"

22) Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

23) Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

24) Page 12 line 33. Provide additional clarity on "monitor". Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

25) Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

26) Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

27) Page 16 line 25, replace “should” with “may”.

Likes 0	
Dislikes 0	

Response

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick

Answer	No
Document Name	

Comment

Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

Requirement R1 needs to be vendor focused. It is not appropriate to assign risk based on the categorization of BES Cyber System impacted by the procurement. This Standard is for supply chain management, not BES Cyber System management. The guidance should not be limited to a brief discussion of Black Energy. To the contrary, the risks presented by Havex appear to be the stronger driver of need as perceived by FERC. It is imperative that vendor risk management controls, such as those cited on Page 4, starting at Line 13, comport with the substantively same or similar requirements of other CIP Standards before being allowed. The Guidance should also address the situation where the Registered Entity has chosen a patch source, per CIP-007-6, Requirement R2, that is not the originator of the software. For example, where the Registered Entity chooses to get its Microsoft and Linux patches from its SCADA/EMS vendor. Some sort of integrity chain needs to be verified.

Likes 0	
Dislikes 0	

Response
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich

Answer	No
Document Name	

Comment
See comments submitted by Black Hills Corporation

Likes 0	
Dislikes 0	

Response
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment
The Technical Guidance Document is well-written based upon what the NERC Drafting Team had to work with, but the controls recommendations within this document are expansive enough to become its own industry. This would be an excellent document to use as a starting point of conversation with our hardware and software supply chain, but to impose it on the Entities as the end customers of these ICS products and applications would be overly burdensome with very little return on investment. This would be particularly true for those Entities dealing only with Low Impact BCS.

Likes 0	
Dislikes 0	

Response
Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment
GTC recommends the SDT consider GTC's comments above, and adapting the Technical Guidance and Examples document accordingly.

Likes 0	
Dislikes 0	

Response	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	
Some of the Technical Guidance and Examples reads more like implementation guidance and other parts sound more like Guidelines and Technical Basis, which should be worked out before industry can adequately provide comments. Also, due to our concerns with the requirements, this document will need to change as well.	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	No
Document Name	
Comment	
R1: The Compliance Guidance states: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.” What qualifies as an existing contract? Is there an obligation to implement the risk management plan when: (1) negotiating and executing a new Statement of Work; (2) negotiating an amendment to a Master Agreement; or (3) renewing a contract under existing terms? The answer to these questions should be clarified and directly addressed in the standard or in the implementation plan. Please clarify how existing versus new procurement elements are addressed, especially for R3 and R4 technical controls.	
Likes 0	
Dislikes 0	
Response	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

Some of the Technical Guidance and Examples reads more like implementation guidance and other parts sound more like Guidelines and Technical Basis, which should be worked out before industry can adequately provide comments. Also, due to our concerns with the requirements, this document will need to change as well.

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

As the *Technical Guidance and Examples* is not legally enforceable LCRA cannot rely on it as an authoritative source for guidance on complying with CIP-013.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC

Answer	No
Document Name	

Comment

SDG&E agrees with EEI comments and proposed language.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	

Comment

Tacoma concurs with the comments provided by the LPPC.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Some of the Technical Guidance and Examples reads more like implementation guidance and other parts sound more like Guidelines and Technical Basis, which should be worked out before industry can adequately provide comments. Also, due to our concerns with the requirements, this document will need to change as well.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

SMUD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

SMUD requests clarification on the term “supplier” as it is used in the guidance document. SMUD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, SMUD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. SMUD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced SMUD requests that the SDT define the term and place it in the NERC Glossary of Terms.

SMUD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. SMUD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, SMUD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment

The NYPA Comments

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA agrees with comments submitted by American Public Power Association.

Likes 0	

Dislikes 0	

Response

Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	

Comment
FEUS supports the comments submitted by APPA

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	

Comment
Seattle City Light requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging. Seattle City Light requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards. Seattle City Light requests clarification on the term “supplier” as it is used in the guidance document. Seattle City Light requests replacing with the term vendor or providing clarification on the difference between the two. In the guidance document on page 6, line 1, Seattle City Light requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.” The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. Seattle City Light requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced Seattle City Light requests that the SDT define the term and place it in the NERC Glossary of Terms. Seattle City Light requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. Seattle City Light requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities. Additionally, Seattle City Light requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	

Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment
R1: The Compliance Guidance states: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.” What qualifies as an existing contract? Is there an obligation to implement the risk management plan when: (1) negotiating and executing a new Statement of Work; (2) negotiating an amendment to a Master Agreement; or (3) renewing a contract under existing terms? The answer to these questions should be clarified and directly addressed in the standard or in the implementation plan. Please clarify how existing versus new procurement elements are addressed, especially for R3 and R4 technical controls.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	

Comment
CSU requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging. CSU requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards. CSU requests clarification on the term “supplier” as it is used in the guidance document. CSU requests replacing with the term vendor or providing clarification on the difference between the two. In the guidance document on page 6, line 1, CSU requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CSU requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CSU requests that the SDT define the term and place it in the NERC Glossary of Terms.

Colorado Springs Utilities (CSU) requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CSU requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CSU requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

1) The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

2) The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or, define the term.

3) Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

4) Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be either defined in this standard or in the NERC Glossary of Terms. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition. The “threatened, attempted” part of this definition would is too large in scope and could require large vendors like Microsoft or Cisco to report thousands or millions of attempts each day. Suggest replacing “vendor security event” in R1.2.1 with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

5) Page 6, line 12: It is unclear that the R1.2.1 requires notification by the entity to the vendor.

6) Suggest adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

7) In other standards, the Guidelines and Technical Basis document is included in the standard, suggest that this also be completed for CIP-013.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA proposes the “Supply Chain” requirements should be clear on what is to be done during the procurement process. Any aspects of service or ongoing maintenance activities should be addressed in the appropriate CIP standard. All requirements for Low impact systems should be in CIP-003.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

As the *Technical Guidance and Examples* is not legally enforceable, LCRA cannot rely on it as an authoritative source for guidance on complying with CIP-013.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper suggests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging.

Santee Cooper requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

Santee Cooper requests clarification on the term “supplier” as it is used in the guidance document. Santee Cooper suggest using consistent terms between the standard and the Technical Guidance.

In the guidance document on page 6, line 1, Santee Cooper requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. Santee Cooper requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset.

Additionally, Santee Cooper requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The Technical Guidance and Example language states, “Entity processes for addressing software risks and vendor remote access risks per Requirements R3 and R4. Consider whether to include low impact BES Cyber Systems in these processes, or alternatively develop a separate cyber security policy or process(es) to address low impact BES Cyber Systems.” R5 states that Responsible Entities must have “one or more documented cyber security policies.” IPC would like to know why the Technical Guidance and Examples language directs Responsible Entities to consider developing “processes” to meet a requirement that explicitly states that Responsible Entities must have “one or more documents cyber security policies” to meet the requirement?

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016.

The entire standard addresses supply chain risk management and therefore should address the possible risks and possible controls for entities to consider for each stage of the life cycle of a system in which there is interaction with and dependence on vendors, their products, and/or their services. These may include but are not limited to evaluation of design, procurement, acquisition, testing, deployment, operation, and maintenance. Reclamation recommends the technical guidance document provide examples of risks and their respective controls (such as contract clauses) for entities to consider.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE

Answer	No
Document Name	

Comment

1. Please include guidance on expectations for resource and time to support the requirements. Most low impact entities do not have a procurement office or manager and are wondering who should be hired or trained to support the supply chain issues.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli

Answer	No
Document Name	

Comment

Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
This document identifies some shortcomings, pitfalls, and/or unintended consequences of prescribing requirements within a mandatory reliability standard and is evidence that a Reliability Standard may not be the best vehicle to address the complexities and broad range of individual Registered Entity nuances in process and infrastructure, on top of the host of jurisdictional, technical, economic, and business relationship issues associated to supply chain; and further demonstrates the essentiality of reconsidering the need for CIP-013-1.	
Likes 0	
Dislikes 0	
Response	

Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	
OUC requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging. OUC requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards. OUC requests clarification on the term “supplier” as it is used in the guidance document. OUC requests replacing with the term vendor or providing clarification on the difference between the two.	

In the guidance document on page 6, line 1, OUC requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. OUC requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced OUC requests that the SDT define the term and place it in the NERC Glossary of Terms.

OUC requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. OUC requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, OUC requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

(Page 2, lines 2-3) An entity should define its specific approach to the SCRM plan in the preamble, so the Regional Entity will be able to evaluate the development and application of the plan.

(Page 2, lines 16-24: This passage gives entities a huge pass on implementation. As long as the entity asked the vendor to play nice during the RFP process, it appears the entity may not be found in noncomoliance if the final vendor contract does not include part or all of the entity's SCRM RFP clauses. This means it will be important to evaluate both the RFP and the final Service Level Agreement [SLA]/Contract for a specific applicable BCS. This review may lead to Recommendations and/or Areas of Concern [AoC], but might be difficult to substantiate Possible Non-Compliance [PNC] Finding as long as the RFP process aligns with the entity's SCRM plan.

(Page 2, line 37). This is true only if such actions are specified in the vendor's SLA.

(Page 3, lines 9-10). This was discussed on an earlier SCRM SDT call, if a vendor can demonstrate that it is certified by ISO or some other certification organization, it may provide a statement to that effect, in lieu of specific agreements with each customer. This issue may still be fluid, but should be included in the final Guidance, as well, in order to satisfy FERC's directive to not extend CIP-013-1 beyond the purview of Section 215 to vendors.

(Page 3, lines 29-30). It appears the key element in this passage is to ensure entities have implemented a sound SCRM program and suitable processes to mitigate vendor risk, it does not require entities to take extraordinary measures to ensure all such processes are included in final SLAs.

(Page 3, lines 42-44) We can reasonably expect most, if not all, SCRM plans to follow the guidelines below to incorporate applicable controls into the plan. However, these suggested controls are best practices, but not mandatory controls. Entities can use these guidelines as an initial starting point for the development of the SCRM plan, as can the Regional Entities for review and evaluation of the R1 SCRM plan at audit..

(Page 4, footnote 1). This footnote cites a third party commercial product. WECC's approach to maintaining auditor independence includes its position to never endorse, recommend, or otherwise indicate favorite vendor status to any consultant, vendor, or product. As a result of this approach, WECC does not consider it appropriate to recommend or endorse a specific tool such as this product.

(Page 5, lines 34-37). This bullet addresses the potential for contractual controls for SCRM that stems from a sound RFP process and procedures. If an entity takes this approach, WECC would expect to see an RFP template that includes specific cyber security terms and expectations. We would then sample for completed RFPs to evaluate the entity's implementation of this approach.

(Page 6, Section 1.2.1 line 4). Unless these processes are specifically included in a vendor SLA or other binding document, it will be difficult for a Regional Entity to evaluate anything other than the entity's plan for such notifications. Since the burden of proof cannot be passed along to the vendor other than through contract, the audit of most of these 1.2.x sections may generally be nothing more than a review of the entity's plan.

(Page 10, lines 6-7). Communications and training materials relative to SCRM should also be addressed in the entity's overall Cyber Security Awareness program.

(Page 13, R4). As mentioned in the R4 comments above, this is a major security concern from WECC's perspective and should leverage and expand upon an entity's controls and procedures for Interactive Remote Access [IRA] from CIP-005-5 R2.

(Page 16, R5). An entity can leverage its R3 and R4 controls to support R5, but it is not required to do so. However. based on prior discussions with entities relative to CIP-010-2 R4, in practice, WECC would expect to see implementation efforts of this nature relative to SCRM controls for Low-impact BCS.

Likes 0	
Dislikes 0	

Response

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Currently, implementation guidance is imbedded in the Technical Guidance document covering what the Standard means, and how to implement it. Southern requests that those topics be separated out.	
Likes 0	
Dislikes 0	
Response	

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	

PSEG appreciates the standard drafting team's effort in providing technical guidance and examples to provide additional clarity and implementation support for the registered entities. PSEG has the following questions/recommendations to the Technical Guidance and Examples document below:

- The term vendors as used in the standards is defined (Page iv Line 6) in the Technical Guidance and Examples document (as well as in the Rationale for Requirement R1 in the draft CIP-013 Standard). This term should be officially defined in the Glossary of Terms used in NERC Reliability Standards.

- Page 4, line 37: Add the wording "as determined by the Registered Entity" after the word components. The new statement would state, "Define any critical elements or components, as determined by the Registered Entity, that may impact the operations or reliability of BES Cyber Systems". This change aligns with the FERC order (p31) statement that the standard should have flexibility to account for varying " differences in the needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risks" to determine the critical elements and components that may impact operations or reliability of BES Cyber systems based on the registered entities implementation of a vendor system or component within their program.

- Page 5, line 24: Add the wording "as identified by the Registered Entity" after the word "risks". The new statement would state, "Review and address other risks as identified by the Registered Entity in Requirement R1 Part 1.1.1." Recommend this change to align with the change to technical guidance for Requirement 1.1.1 (Page 4, line 37) above.

- Page 6, line 43: Replace the word "breaches" with "vulnerabilities and threats" to align with the use of the word "vulnerabities" in the requirement language.

- Page 7, line 1: Replace the word "breach" with "vulnerability" to align with the use of the word "vulnerabities" in the requirement language.

- Page 7, line 9: Remove the words "availability or". The NERC CIP reliability standards require protecting BES Cyber Systems to support reliable operation of the BES. Recommend removing availability to align with the wording used throughout the NERC CIP reliability standards.

- Page 13, line 9: Recommend changing Requirement 4.3, from "Disabling or otherwise responding to unauthorized activity during remote access sessions"to "Disabling or otherwise responding to detected unauthorized activity associated with remote access sessions." (see comment under question 4)

- Page 15, line 22: Recommend adding the word “detected” to align with the recommended changes to Requirement 4.3. The statement would become “Set up alerting and response processes so that detected inappropriate vendor remote access sessions may be disabled or otherwise responded to in a timely manner.

- Page 15, line 23: The words “in a timely manner” are overly subjective. Recommend specifying a specific time frame for a timely response.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	

Comment

AZPS requests clarification that the Technical Guidance and Examples being incorporated into the Standard will be used as technical guidance only, and not compliance guidance.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
There is inconsistency with the language of the Requirements and the Technical Guidance language, specifically in reference to Requirement R3 and Requirement R4. The guidance sections for both Requirements mention reviewing security policies, however, the Requirements mention Risk Management Plans. NRG suggests that this language be properly aligned or else this could lead to future Compliance Enforcement issues for the industry. NRG requests SDT clarity that system-to-system is equivalent to machine-machine.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	

On Page 9, line 43, the Technical Guidance and Examples references the use of industry best practices and guidance that improve cyber security risk management controls. This does not match the rationale of R2 which only speaks to the use of guidance. Exelon feels that the reference to “industry best practices” should be removed from the Technical Guidance and Examples since it is non-specific and open to interpretation.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	
Document Name	

Comment

The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or, define the term.

Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be either defined in this standard or in the NERC Glossary of Terms. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition. The “threatened, attempted” part of this definition would is too large in scope and could require large vendors like Microsoft or Cisco to report thousands or millions of attempts each day. Suggest replacing “vendor security event” in R1.2.1 with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Page 6, line 12: It is unclear that the R1.2.1 requires notification by the entity to the vendor.

Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”.

Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”.

Page 11, Line 15, replace supplier with Vendor.

Page 11, line 25, replace “should” with “may”

Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

Page 16 line 25, replace “should” with “may”.

Suggest adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging

In other standards, the Guidelines and Technical Basis document is included in the standard, suggest that this also be completed for CIP-013.

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE has no comments for this question.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant

Answer	

Document Name	
Comment	
We did review the TG&E document briefly and it was valuable in illustrating how some of the team members were viewing various requirements; however, it will need to be further refined once the changes are made to the requirements. We did note that in the discussion of integrity and authenticity, there was a lot of duplication in methods between the two making it seem that there might be some fuzziness on what each of the two descriptors are trying to address.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	
Document Name	
Comment	
- See APPA's comments.	
Likes 0	
Dislikes 0	
Response	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Response	
Glenn Pressler - CPS Energy - 1	
Answer	

Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	

9. Provide any additional comments for the SDT to consider, if desired.

Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	

In voting “no” on this proposed Reliability Standard, MRO acknowledges the impossible challenge faced by the Standard Drafting Team and NERC in developing a Supply Chain Reliability Standard as directed in FERC Order No. 829 issued July 21, 2016. Federal Energy Regulatory Commission (FERC) Acting Chairman LaFleur (then a commissioner), stated in her dissenting opinion, “[E]ffectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, economic, and business relationship issues.”

As a regulator, MRO seeks to provide clarity about Reliability Standard requirements, assurance around compliance with those Reliability Standards, and results – reduced risk to the reliable operation of the bulk power system (BPS). Adoption of the proposed Reliability Standard will not meet these goals.

The proposed Reliability Standard directs registered entities to complete tasks that require agreement of vendors that are not subject to the jurisdiction of the FERC or the Electric Reliability Organization (ERO). To accommodate this lack of jurisdiction, the proposed Reliability Standard is drafted sufficiently vague to allow for lack of vendor agreement and compliance with the Reliability Standard to exist at the same time. For example, Requirement 1 of CIP-013 obligates registered entities to implement supply chain risk management plans. At the same time, the supporting Rationale states, “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement the entity’s plan.” In essence, this Requirement forces entities to develop a plan, but a failure to be able to implement the plan is not an issue of noncompliance. The root cause of the problem is that the risk lies with vendors, a third party not subject to FERC or ERO jurisdiction. Thus, the Reliability Standard becomes more paperwork and administrivia than mitigation of risk. See the comments of the MRO stakeholder-driven NERC Standards Review Forum.

As a regulator, MRO believes the proposed Reliability Standard cannot be effectively and efficiently assessed and therefore MRO would not be able to provide assurance of compliance or, more important, assurance of reduced risk to the reliable operation of the BPS. As drafted, MRO will be expected to determine if registered entities made a reasonable attempt to address supply chain risks through their procurement processes. Since contracts are always a give and take with regard to a number of provisions, how does a regulator efficiently and effectively monitor one aspect of the contract negotiation process to determine reasonableness and the possible existence of countermeasures to address security throughout the procurement process which may be beyond our jurisdiction and rest with best security practices?

In addition, the draft Reliability Standard does not address supply chain management comprehensively. For example, the issues associated with vendors of the vendors are not addressed. It is very common for an Energy Management System (EMS) vendor to deliver a system with third party software, such as Adobe®, Java, or even open-sourced software such as PuTTY. The vendor chain for any system can be deep and the proposed Reliability Standard does not provide registered entities clarity on how to deal with these routine layers of vendors.

Finally, it is also important to consider the potential economic impact on future contract negotiations between registered entities and vendors. The proposed CIP-013 directs a registered entity to address supply chain risks in its vendor contracts. How much does the registered entity pay to manage supply chain risk when the vendor has no legal obligation to accommodate the registered entity? By placing additional requirements on vendors, do we unintentionally reduce competition, increase costs, and reduce innovation? Furhtermore, the possibility of less competition, creates less diversity across the bulk power system and less diversity increases risk.

Reducing supply chain risk to the reliable operations of the BPS and providing the requisite regulatory assurance that that risk has been reduced is a complex task for the very reasons FERC Acting Chairman LaFleur communicated in her dissent. Whether or not this risk is best addressed by a NERC Reliability Standard as opposed to a security framework, an IEEE standard or use of military grade components merits greater consideration. This is particularly true given four of the five FERC commissioners will have either not considered or not supported FERC Order 829 when the proposed Reliability Standard is ultimately filed with FERC. Following the comment period, MRO recommends that FERC and the ERO consider whether we have

the appropriate structure and expertise to address and mitigate this risk that resides with vendors effectively and efficiently through a Reliability Standard.	
Likes 2	Platte River Power Authority, 5, Archie Tyson; Gresham Darnez On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1,
Dislikes 0	
Response	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The NSRF has concerns with being held accountable for a vendor who does not meet the attributes of this proposed Standard, especially for entities that have Low Impact BES Cyber Systems, only. Many of the entities that have Low Impact BES Cyber Systems only, are small (read low risk) entities that may have one Low Impact BES Cyber Systems (maybe a generator, one Transmission substation, or control system). How is the small entity going to stand up to large multi-regional corporate companies (i.e. the vendor), when the vendor will not comply with the requirements of the small entity (and CIP-013-1)? The Low Impact BES Cyber Systems entity will carry all the compliance risks (burden) when they find out that the vendor did not comply with said requirements, regardless of how the entity will ensure that the vendor will comply, a contract, statement of work, etc. If the vendor does agree with supplying proof that is requested, the small entity will then incur **more cost** (read increase costs) to the Low Impact BES Cyber Systems entity by being found non-compliant. The entity may not be able to recoup that cost due to the rate structure of that entity's state commission. This may lead the small entity to assume more risks because the cost is too great and not have a system fully protected. They would be fully compliant by writing their plan and stating everything is low risk and controls are not required. The guidance document suggests not making these requirements contractual language as it makes negotiations more difficult. This puts us in a poor situation as we are required to do it but don't get NERC support via a requirement in the standard to force the agreement to stipulate it. If it was part of the standard to require it, it would give all Responsible Entities consistent leverage to utilize as all would require it. NERC should provide the areas that should be covered in an agreement in a standard format to provide consistency. The Standard does not make it clear how any cloud based services may be impacted by this standard. We suggest the SDT to consider how this standard may apply to cloud based systems and provide any relevant clarifications.	
Likes 2	Platte River Power Authority, 5, Archie Tyson; OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	

No additional comments.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	
Document Name	

Comment

We are concerned that CIP-013-1 may oblige entities to purchase equipment that doesn't presently exist and may never exist, and to take actions that are impossible. The standard should at a minimum state that it does not require NERC entities to:

- impose cyber security measures or reporting on the suppliers of programmable electronic devices (PEDs),

- monitor vendors to ensure that they are properly implementing their cyber security programs,

- ensure that as-received software and firmware is in the as-shipped condition.

- eliminate risk (only mitigation of risk is possible).

It would be impractical for vendors to individually negotiate a unique CIP agreement with each purchaser, and the net effect on BES reliability could be negative if the current vendor (for NERC entities with standardization programs) or the vendor with the best product (for competitive bidding) chooses not to develop CIP-013-friendly products due to the burden of compliance. We would support a qualification program administered by a NERC-approved central authority, however, such that entities could address supplier-related issues simply by purchasing CIP-013-certified products.

A blanket allowance is needed for entities to take technical feasibility exceptions (TFEs), to address the wide variety of PED types and to address instances of vendors not producing the inputs that entities are supposed to act upon.

CIP-013-1 as presently written may create extreme reluctance to enhance plants in accordance with technological developments, which again would be counterproductive regarding long-term BES reliability.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	
Document Name	

Comment

See APPA's, TAP's, and USI's comments.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 5

Answer	
Document Name	

Comment

AEP believes the SDT should specifically mention CIP Exceptional Circumstances in the Standard in order to clearly identify that entities would be exempt from complying with CIP-013-1 in the event of a qualifying CIP Exceptional Circumstance.

In addition, Order 829 specifically mentions that the Standard should be forward-looking, but CIP-013-1 does not mention it. AEP believes the SDT should revise CIP-013-1 to include a statement in alignment with FERC's directive that this Standard should be forward-looking.

Likes 0	
Dislikes 0	

Response

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3

Answer	
Document Name	

Comment

Please modify this standard using the similar 'Applicability' table format used in the earlier standards.

This set of base requirements is would duplicate effort on the part of each entity to evaluate Supply Chain risk for vendors that provide the same product to multiple entities. Some consideration should be given to creating a standard review, application or qualification form that vendors can complete to certify their product and its delivery.

Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	

There is significant overlap to CIP-005, 007, 008, 010. If the intent is to impose additional requirements on the procurement process those requirements should be integrated into the appropriate standard to maintain the linkage. Duplication of requirements in another standard will only create confusion and wasted effort for entities to meet CIP compliance.

The requirements as written are not consistent with the standard's stated purpose: "To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems." This purpose statement indicates this standard is intended to address items that should be considered during the procurement/contract negotiations process and included in terms of the contracts. The requirements as written imply that enforcement of the terms of the contract will be audited. The lifecycle management is currently addressed in CIP-005, 007, 008, 010.

The applicability of each of the requirements is not clearly addressed. Standards CIP-002 through CIP-011 clearly define the applicability for each requirement and sub-requirement.

2. Suggest include supply chain certifications such as ISO-28000 and Customs-Trade Partnership Against Terrorism certification as items to ask for in request for purchase.

Likes 0	
Dislikes 0	
Response	

Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	
Response	

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	
Document Name	

Comment
R1.2.6 states the RE needs to provide "*Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s);"* While R4 and R5 require *"Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s)."* Different terms regarding obligations for vendor remote access have been used with regard to R1.2.6 than under R4 and R5 (e.g., "coordination" and "controlling:"). We seek clarification on whether that is intentional. If the two terms are intentionally different, more clarity is needed on what different obligations are being imposed between R1.2.6 and R4/R5. If R1.2.6 and R4/5 are not meant to impose different obligations, we suggest use of consistent terms or wording.

Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	

Comment
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	
Document Name	

Comment

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CHPD feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CHPD if this was intentional for R3 and R4. CHPD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	
Document Name	

Comment

PRPA understands that the SDT is under time constraints in addressing Order No. 829, however, PRPA requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

PRPA requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

PRPA feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to PRPA if this was intentional for R3 and R4. PRPA requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	
Document Name	

Comment

AE understands that the SDT is under time constraints in addressing Order No. 829, however, AE requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

AE requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

AE feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to AE if this was intentional for R3 and R4. AE requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	

Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standard.

Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments including modifications to existing contracts and agreements to deliver desired solutions. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

Moify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

Move CIP-013 R2 into CIP-003-x R1 with other CIP policies that are reviewed by the CIP Senior Manager. This would also provide alignment across high, medium, and low impact Cyber Assets.

CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	
Document Name	
Comment	

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	
Document Name	

Comment

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CHPD feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CHPD if this was intentional for R3 and R4. CHPD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Response

W. Dwayne Preston - Austin Energy - 3

Answer	
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Response	

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	
Document Name	
Comment	
As written, implementation of this draft standard may degrade rather than improve reliability by interfering with the ability to respond and recover from BES cybersecurity events. The draft standard also encourages the use of a monoculture of products allowing broader damage from a single zero-day vulnerability.	
Likes 0	
Dislikes 0	
Response	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Response	

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable

Answer	

Document Name	

Comment

The American Council of Engineering Companies (ACEC) -the business association of the nation's engineering industry - wants to convey the industry's perspectives and concerns over the development of this new cyber security supply chain rule mandated by the Federal Energy Regulatory Commission (FERC).

ACEC member firms, numbering more than 5,000 firms representing over 500,000 employees throughout the country, are engaged in a wide range of engineering works that propel the nation's economy, and enhance and safeguard America's quality of life. Council members are actively involved in every aspect of the energy marketplace.

Supply chain cyber security is of growing concern to all our members. While we believe that present cyber security controls and voluntary practices are highly effective, input by engineering service providers would assist NERC/FERC in producing a more effective approach in minimizing the impacts on competition, risk allocation, and pricing.

In short, ACEC is in agreement with most of the comments of the owners, operators, vendors and suppliers that have formally participated in this Standard development. We fully appreciate the concerns over how risk can be adequately managed under any proposed standard. Our member firms' reputations depend upon professional performance and innovation in an atmosphere of collaboration. However, we are concerned that the supply chain language in this Standard will not support, and may actually impair, broad-based cost-effective infrastructure security and grid reliability

Likes 0	
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	
Document Name	

Comment

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor’s inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CHPD feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states “suppliers, vendors and other entities”. The Requirement language only references vendors. The SDT should clarify who or what “suppliers” and “other entities” are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CHPD if this was intentional for R3 and R4. CHPD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

SRP understands that the SDT is under time constraints in addressing Order No. 829, however, SRP requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

SRP requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor’s inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

SRP feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states “suppliers, vendors and other entities”. The Requirement language only references vendors. The SDT should clarify who or what “suppliers” and “other entities” are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to SRP if this was intentional for R3 and R4. SRP requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	
Document Name	
Comment	
FirstEnergy recommends that the SDT take additional time in preparing a draft supply chain Standard that properly separates “supply chain” Requirements from additional operational and maintenance Requirements. Operational and maintenance Requirements should be added to the existing CIP Standards where the subject protections are already addressed. In addition, any Requirements applicable to Low Impact BES Cyber Systems should be placed in CIP-003 as has been established as a practice for all other low impact requirements. It should also be noted that certain expectations of these Requirements have economic implications to entities of all sizes. These Requirements could result in limiting the flexibility of an entity to obtain cyber assets from third-party distributors at a significant discount. For some entities, the additional costs could have an impact on their ability to remain for example, an economically viable generating unit. While probably not something that by itself impact the continued operation of a generating unit, the additional costs associated could be an influencing factor in keeping BES generating unit in-service.	
Likes 0	
Dislikes 0	

Response
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1
Answer	
Document Name	
Comment
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).
Likes 0	
Dislikes 0	
Response
Mike Kraft - Basin Electric Power Cooperative - 5
Answer	
Document Name	
Comment
Basin Electric has concerns with being held accountable for vendors who not meet the attributes of this proposed Standard. Basin Electric prefers existing CIP standards be modified to satisfy the order. With the current FERC Commission lacking quorum, the timeframe to add commission members and the resulting backlog from the delay, it would appear the FERC Commission is not in a position to act upon a hastily constructed new standard. Basin Electric suggests NERC request an extension of time to modify existing standards to meet the order. Basin Electric suggests CIP-013 follow the table structure used in the existing enforceable CIP standards including the Part, Applicable Systems, Requirements and Measures.
Likes 0	
Dislikes 0	
Response
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison
Answer	
Document Name	
Comment

Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

Move CIP-013 R3, to CIP-010 R1.

CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

Move CIP-013 R5 to CIP-003 R2

Question – what about contracts negotiated during the implementation period? Are these contracts subject to this Standard? What about existing contracts? What about contracts that are renewed (evergreen contracts)? What about contracts initiated during the 15 calendar month review?

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	
Document Name	

Comment

Seminole Electric comments submitted by Michael Haff

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx

Comment
See comments in the attached file.

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	
Document Name	

Comment
PJM agrees with the comments submitted by the SWG. Additionally, PJM suggests that 1.2.1 be stricken since it is ambiguous and already covered by 1.2.3 and 1.2.4. It is not clear what would be defined as a “vendor security event” that is outside of the events listed in 1.2.3 and 1.2.4.

Likes 0	
Dislikes 0	

Response

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	
Document Name	

Comment
“This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement.” - Verbiage to this effect needs to be part of the standard. Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event. Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	
Document Name	

Comment

Verbiage similar to the follwoing needs to be part of the standard. “This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement.”

Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event.

Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	
Document Name	

Comment

Summary of comments direction:

1. No “plans.” (Delete R1 and R2). Order 829’s four objectives did not include creating “plans.”

2. All four of the directives either direct or use examples of specific operational cyber security controls which are best addressed as revisions to CIP-002 through -011. (Delete R3-5).

3. We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives' deadlines, NERC and industry should reprioritize SDT teams' work and resources.

Result: No CIP-013 standard. Revised CIP-002 through -011 standards.

Other comments:

On the one hand Order 829 states intent to respect FPA section 215 jurisdiction by only addressing the obligations of responsible entities. A Reliability Standard should not directly impose obligations on suppliers, vendors or other entities that provide products or services to responsible entities.

Yet, in paragraph 59, Order 829 states, "The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations."

Contracts are bi-lateral and as such impose obligations on both parties, in direct contradiction to not imposing obligations on suppliers, vendors or other entities. Paragraph 59 is indirectly imposing obligations on suppliers, vendors or other entities that provide products or services to responsible entities.

If the entity chooses, contracts can be a tool in "how" they deliver the "what" for the security objective. However, the registered entity's compliance has to be measured on achieving the security objective, not on contract terms.

We will not support any standard that prescribes contract terms and makes contract terms a measure of an entity's compliance. Entities have been achieving the CIP-004 security objectives for background checks, training and access revocations since CIP version 1 without the prescription of "how" it had to be done (without making contract terms a measure of their compliance).

We strongly agree with the Midwest Reliability Organization comments.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	
Document Name	
Comment	

"This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement." - Verbiage to this effect needs to be part of the standard.

Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event.

Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	
Document Name	
Comment	

- During the Assess/Plan, Procure/Acquire phases of the Supply Chain process, separate requirements for standalone Standard (CIP-013) should be developed. For the deployment and operational aspects of the Supply Chain, appropriate requirements should be incorporated into the existing CIP Standards. It is recommended that this SDT collaborate with the CIP-002-CIP-011 SDT for language that can be used until R3 – R5 can be moved to their appropriate operational standards.
- All measures sections will need to be updated to reflect any changes that are made to the requirements.
- Dominion recommends that "remote access" should be changed to "electronic remote access" throughout the proposed CIP-013-1.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	
Document Name	

Comment

The need to have supply chain risk management is agreeable; however, in its current form, CIP-013-1 poses a great challenge and burden to SCE&G and other Responsible Entities for various reasons, many of them documented in the Unofficial Comment Form. SCE&G recommends that CIP-013-1 include a modified R1 and R2 only, and not include R3 through R5. Requirements R1 and R2 focus on the supply chain and will suffice as an initial implementation step of supply chain risk management. The remaining requirements are operational obligations that need to be integrated into existing NERC CIP Standards.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	
Document Name	

Comment

Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standards.

Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Also recommend the following:

- Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.
- Move CIP-013 R3, to CIP-010 R1.
- CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6
- Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5

Answer	
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6

Answer	
Document Name	

Comment

Request verbiage similar to the following is added as part of the standard:

This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement.

Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event.

Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	
Document Name	

Comment

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	
Document Name	

Comment

{C}1) Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

{C}2) This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

{C}3) As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standard.

{C}4) Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

{C}a. Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

{C}b. Move CIP-013 R3, to CIP-010 R1.

{C}c. CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

{C}d. Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

In the Purpose, change “security controls” to “procurement and operational controls” as presented in the materials.

CenterPoint Energy request that the SDT format CIP-013 like the other CIP Standards, a table design, if possible.

CenterPoint Energy suggests more collaboration between the CIP Modifications SDT and the Supply Chain SDT to help eliminate overlap and better align with existing CIP requirements.

In general, the SDT should consider the operational impacts that this standard could have on the industry. Flexibility is necessary.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	
Document Name	
Comment	

HQT voted Negative and would like to see the following matters to be addressed:

-CIP-013 should move forward with only R1 and R2 since they are mostly procurement related-some concern is being expressed that the requirements for having a supply chain risk management plan seem to a cover low medium and high BES Cyber assets as well as allowing entities to assess their own risk. Further clarification and perhaps some third party verification would be beneficial.

-Contractual issues could exist. Although the FERC order doesn't require abrogation of contracts there is some concern that there could end up being multiple contracts in place, those newly negotiated and the existing ones. Confusion exists between use of terms vendor and suppliers in the draft standard and the Guidance section.

-Concerns exist regarding authentication on multiple levels and how vendors and their manufacturers may combine hardware and software into their products and how there could meaningful verification and authentication

-There are a number of areas where time seems to be an issue as it relates to implementation

-Use of "applicability tables" as they appear in other CIP standards would clarify the requirements to alleviate compliance concerns

- R3, R4 and R5 should move into existing CIP Standards to avoid P81 issues (redundancies) and ease implementation for Entities and improve auditability efficiencies.

Likes 0	
Dislikes 0	
Response	

Ballard Mutters - Orlando Utilities Commission - 3	
Answer	
Document Name	
Comment	

OUC understands that the SDT is under time constraints in addressing Order No. 829, however, OUC requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

OUC requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	
Document Name	

Comment

In conclusion, ATC has concern that, despite what is a well-intended attempt by a highly qualified SDT to address the directives of FERC Order 829, CIP-013-1 is its current form is ultimately serving as an vehicle to revise or expand the scope and requirements to several currently approved and enforceable CIP Cyber Security Reliability Standards without affording the industry due process in accordance with the NERC Rules of Procedure for those modifications. 1.) Where existing Reliability Standards and Requirements meet the intent of CIP-013-1 and the FERC Order 829 directives, the existing Reliability Standards should be leveraged to accomplish the objective instead of creating a duplicative standard. 2.) Where Reliability Standards and Requirements may not go far enough to meet a given objective as it relates to vendors or suppliers, consideration should be given to modifying those existing Reliability Standards and Requirements, or perhaps investing time toward the further exploration of leveraging available standardized industry frameworks or practices that meet the objectives in an ever changing threat landscape as opposed to a reliability standard that a.) may be ill-equipped to keep pace with emerging threats and b.) perhaps carry the risk of hindering a Registered Entity's ability to be timely and nimble in addressing those threats in order to maintain compliance with a requirement(s) that has been rendered irrelevant. The creation of a new Reliability Standard should not supersede, contradict, expand, amend, or otherwise effectively revise other currently approved and enforceable CIP Cyber Security Reliability Standards. Those Standards exposed to this condition are cited in other comments and include, at a minimum the below listed five (5) CIP Standards:

- CIP-002-5.1
- CIP-003-6
- CIP-004-6
- CIP-005-5
- CIP-007-6

In conclusion, the above concerns related to redundancy or contradiction to approved and enforceable CIP Standards, the cited expansion to the FERC directives, and the confusion, inconsistency, and broad sweeping language that is at odds with the intent of both enforceable CIP Standards, the effort of paragraph 81, and FERC Order 829 supports the wisdom and caution within FERC Commissioner's (Cheryl A. LaFleur's) dissent to FERC Order 829. LaFleur's dissent to FERC Order 829. (P. 67) issued on July 21, 2016, cautions that "**…effectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, technical, economic, and business relationship issues**." In this dissent, LaFleur acknowledges that the threat of inadequate supply chain risk management procedures poses a very real threat to grid reliability; and while LaFleur offers full support of the Commission's continued attention to this threat, LaFleur's **"…fear that the flexibility** *[within FERC Order 829]* **is in fact a lack of guidance and will therefore be a double-edged sword.**" is demonstrable in this first draft of CIP-013, and further evidence that FERC Order 829 may have been premature thereby causing a highly qualified and well-intended SDT to be ill-equipped to "**…translate general supply chain concerns into a clear, auditable, and enforceable standard within the framework of section 215 of the Federal Power Act.**" With

Cheryl A. LaFleur's recent appointment to FERC's Acting Chairman on January 23, 2017, ATC respectfully encourages NERC and the SDT to consider if there is an opportunity for FERC to revisit the need for the CIP-013-1 Supply Chain Reliability Standard and to reevaluate the appropriateness and viability of FERC Order 829 and whether or not the SDT should move forward or if FERC Order 829 should be rescinded in favor of the industry leveraging the existing CIP-002 – CIP-011 approved and enforceable reliability standards in combination with the risk-based industry standards and frameworks as an alternative approach to drafting this new Reliability Standard. ATC thanks the SDT for consideration of our positions.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE

Answer	
Document Name	

Comment

1. We believe in finding a beneficial multi-sector solution that will lower costs, encourage innovation, and support among multisector vendors.

2. The current standard would create a compliance burden for entities that are already resource constrained.

3. We believe that the SDT should focus on a supply chain management standard that is designed to:

· Manage in addition to eliminating risk;

· Ensure that operations are adapting to constantly evolving threats;

· Be aware of and responsive to changes within their own organization, programs, and the supporting information systems; and

· Adjust to the rapidly evolving practices of the electricity sector's supply chain.

4. Though the current language would certainly raise standards across the entirety of the software industry, it could result in isolation of the electricity sector and hamper growth and innovation among industrial control vendors.

5. We thank you for the opportunity to comment.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	

Reclamation commends the SDT for the draft that was provided for a new and complex standard in a short amount of time.

Reclamation recommends a more simplified format of the proposed standard.

Reclamation believes that the objectives and intent and of FERC Order 829 can be met without spelling out each objective as a separate requirement. As presently written, the first draft contains repeating elements (such as access, authentication, product delivery, etc.) in different requirements. The simplified approach described in the answers to Questions 1 through 5 above would eliminate redundancy.

Likes 0	
Dislikes 0	
Response	

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	

Santee Cooper understands that the SDT is under time constraints in addressing Order No. 829, however, the SDT should carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

Santee Cooper requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

Santee Cooper recommends that all standards with requirements that apply to low impact assets be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear if this was intentional for R3 and R4. Santee Cooper requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Santee Cooper recognizes the importance of regulatory bodies and the regulatory industry jointly addressing issues concerning cybersecurity and the reliability of the bulk electric system. In this standard, Santee Cooper agrees with other industry comments that many of the gaps addressed in CIP-013 should be modified in other standards and not established as a new standard nearly duplicative of (or worse, in conflict with) other standards. FERC provided NERC the opportunity to either develop a new or modified standard, and Santee Cooper urges the SDT to pursue the latter option as much as is appropriate. Requirements in CIP-013 to address gaps remain must be carefully crafted to avoid creating an ineffective, unauditable and unenforceable standard. Additionally, the short timeframe for submission of this standard and implementation period restricts the utility industry from contributing meaningful and thoughtful comments that would better focus on supply chain concerns that does not advance the security of the grid, as set out by now-Chairperson LaFleur in her dissent to Order 829.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
FERC Order no 829 (p21) discusses “suppliers, vendors and other entities”. CIP-013-1 only refers to vendors. BPA suggests that the SDT clarify the scope and define any appropriate differences applicable to supplier, vendors or other entities.	
Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	

Document Name	

Comment

1) This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

2) As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standard.

3) Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments including modifications to existing contracts and agreements to deliver desired solutions. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

a. Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

b. Move CIP-013 R2 into CIP-003-x R1 with other CIP policies that are reviewed by the CIP Senior Manager. This would also provide alignment across high, medium, and low impact Cyber Assets.

c. CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

d. Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1

Answer	
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	
Document Name	
Comment	

Colorado Springs Utilities (CSU) understands that the SDT is under time constraints in addressing Order No. 829, however, CSU requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CSU requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CSU feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CSU if this was intentional for R3 and R4. CSU requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

CSU requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although

the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
While there are different ways to approach the complex issues of the supply chain risk, a proactive approach to address the issue can only help improve the industry's security posture. The difficulty in addressing the complexities requires additional evaluation to address the issues impacting both the development and implementation of solutions. Similar to CIP-014, the development of Supply Chain Risk Management plans and procurement process proposed under R1 and R2 may be appropriate within a new or revised Reliability Standard. The technical controls proposed for CIP-013 R3 and R4 may be better addressed within existing CIP Standards. The IESO abstains from commenting on R5 but believes integration into existing CIP Standards might be appropriate, especially since CIP-003 Attachment 1 already is comprised of a security plan. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. This is applicable to Requirements 1, 3, 4, and 5. The plan should allow for risk acceptance and leverage of an exception process. To address these concern, the drafting team should include some provisional or exception language to protect Responsible Entities such as use of a Technical Feasibility Exception (TFE). NERC's Appendix 4D to the Rules of Procedure provide for a basis of approval of a TFE beyond strict technical limitations of a system. Reference Section 3.0 of the appendix for more information. The Standard uses "supplier" and "vendor" throughout, interchangeably. The terms should be consistent throughout to avoid confusion.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	CIP-013 Comment Mar 2 revision SCL 2017-3-6.docx
Comment	
The attached document has comments compiled for all the questions. Please note that the BOLD paragraphs below (YELLOW highlighted in attachment) are uniquely Seattle City Lights. The un-highlighted comments were developed in collaboration with other entities and trade organizations such as LPPC. These comments may be like those submitted by other entities but not necessarily. City Light recognizes the challenges facing the SDT and appreciates the efforts the SDT is placing into working towards developing a solid standard.	

Seattle City Light understands that the SDT is under time constraints in addressing Order No. 829, however, Seattle City Light requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

Seattle City Light requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively, this could be addressed as an Exemption in Section 4.2.3.

Seattle City Light feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to Seattle City Light if this was intentional for R3 and R4. Seattle City Light requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

As discussed in comments to R1 above, Seattle City Light requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk.

Seattle City Light recognizes the importance of regulatory bodies and the regulatory industry jointly addressing issues concerning cybersecurity and the reliability of the bulk electric system. In this standard, City Light agrees with other industry comments that many of the gaps addressed in CIP-013 should be modified in other standards and not established as a new standard nearly duplicative of (or worse, in conflict with) other standards. FERC provided NERC the opportunity to either develop a new or modified standard, and City Light urges the SDT to pursue the latter option as much as is appropriate. Requirements in CIP-013 to address the gaps that remain must be carefully crafted to avoid creating an ineffective, unauditable and unenforceable standard. Additionally, the short timeframe for submission of this standard and implementation period restricts the utility industry from contributing meaningful and thoughtful comments that would better focus on supply chain concerns. Thus this standard "does not advance the security of the grid," as set out by now-Chairperson LaFleur in her dissent to Order 829.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	
Document Name	

Comment
FMPA agrees with comments submitted by American Public Power Association.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	Hydro One_Unofficial_Comment_Form_CIP-013-1-First Draft.docx

Comment
We suggest that the standard should have two requirements only. R1 could require the entities to identify risks, evaluate controls (at minimum the controls itemized in FERC Order), and implement controls based on the acceptable level of risk to address the four objectives in FERC Order and mitigate risks stated in the Order. R2 could be the periodic review and approval of R1 by CIP Senior Manager. The applicability could be to all BES Cyber Systems essential for operation of BES. Entities should consider impact rating of High, Medium and Lows when evaluating necessary controls. **Comment for consideration in the RSAW** For the RSAW and under Requirement 1 in the section called “Note to the Auditor”, We recommend adding that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” as stipulated in the Rationale for Requirement 1.

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5	
Answer	
Document Name	

Comment
The NYPA Comments

Likes 0	
Dislikes 0	

Response
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	
Document Name	

Comment
SMUD understands that the SDT is under time constraints in addressing Order No. 829, however, SMUD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1. SMUD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3. SMUD feels that all standards with requirements that apply to low impact assets should be included in CIP -003. As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard. Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to SMUD if this was intentional for R3 and R4. SMUD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

EEI members prefer use of the applicability tables, especially for R3 and R4.

EEI commends the work done by the SDT and NERC on this difficult task. CIP-013 is a challenging standard given it is focused on minimizing risk introduced by third parties that the Responsible Entities have little control over. In particular, we are reminded of Acting Chairman LaFleur's dissenting statement "effectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, economic, and business relationship issues."

In addressing our comments and others, we recommend that the SDT focus on the security objectives and what the Responsible Entities can do in procurement to minimize risk to the bulk-power system. Although cybersecurity is a risk, other risks such as reliability may outweigh the need for certain cybersecurity focused requirements. Cybersecurity is about managing risk, which must be balanced against a number of factors and for the electricity subsector, keeping the lights on is key.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	
Document Name	

Comment

Tacoma concurs with the comments provided by the LPPC.

Likes 0	

Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	
Document Name	

Comment

BANC supports the comments filed by Sacramento Municipal Utility District

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	
Document Name	

Comment

While there are different ways to approach the complex issues of the supply chain risk, a proactive approach to address the issue can only help improve the industry's security posture. The difficulty in addressing the complexities requires additional evaluation to address the issues impacting both the development and implementation of solutions. Similar to CIP-014, the development of Supply Chain Risk Management plans and procurement process proposed under R1 and R2 may appropriate within a new or revised Reliability Standard. The technical controls proposed for CIP-013 R3 and R4 may be better addressed within existing CIP Standards. The IRC abstains from commenting on R5 but believes integration into existing CIP Standards might be appropriate, especially since CIP-003 Attachment 1 already is comprised of a security plan.

This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. This is applicable to Requirements 1, 3, 4, and 5. The plan should allow for risk acceptance and leverage of an exception process. To address these concern, the drafting team should include some provisional or exception language to protect Responsible Entities such as use of a Technical Feasibility Exception (TFE). NERC's Appendix 4D to the Rules of Procedure provide for a basis of approval of a TFE beyond strict technical limitations of a system. Reference Section 3.0 of the appendix for more information.

The Standard uses "supplier" and "vendor" throughout, interchangeably. The terms should be consistent throughout to avoid confusion

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	
Document Name	
Comment	

We appreciate the significant efforts of the SDT to develop this draft standard on difficult subject matter in such a short amount of time. However, based upon this initial draft, it is evident that additional time is necessary for the SDT to develop an effective standard addressing supply chain security risks. We suggest that the SDT develop a formal recommendation to NERC staff requesting that NERC file for an extension of time to collect additional stakeholder feedback in order to develop a more effective standard.

In general, we request that the SDT consider our comments in question 1 that supply the following framework for a supply chain security standard:

FERC's directives in paragraphs 43 through paragraph 62 summarized a general framework for this new Standard as outlined:

R1: Develop a plan to include security controls for supply chain management that include the following four specific security objectives in the context of addressing supply chain management risks:

R1.1 Security objective 3 (*information system planning*)

R1.2 Security objective 4 (*vendor risk management and procurement controls*)

R1.3 Security objective 1 (*software integrity and authenticity*)

R1.4 Security objective 2 (*vendor remote access*)

R2: Implement the plan specified in R1 in a forward looking manner.

R3: Review and update, as necessary its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months

R3.1 Evaluation of revisions…

R3.2 Obtaining CIP Senior Manager or delegate approval.

GTC feels this framework outlined above satisfies Order 829 in the context of addressing supply chain management risks, completely. Although FERC expressed some operational scenarios of existing CIP standards not explicitly addressing supply chain risks, the point of FERC's summary was still in the context of addressing supply chain risks and not additional operational controls as presented by the SDT.

From a clarity standpoint, we urge the drafting team to consider limiting the structure of CIP-013-1 to the supply chain horizon which ends at the delivery of products/services to the acquirer in accordance with NIST SP 800-53 r4 rather than a holistic BES Cyber System Life Cycle approach chosen. GTC submits that the operations and maintenance of BES Cyber systems are already addressed in existing standards. Lastly, FERC provides NERC

discretion per paragraph 44 the option of modifying existing Reliability Standards to satisfy the directive, so if the SDT believes additional operational gaps still exist, then GTC prefers NERC identify these risks, and explain to FERC NERC's intent to invoke operational changes by modifying existing CIP requirements with the submission of a "supply chain horizon contained" CIP-013-1.

Lastly, GTC recommends the SDT develop a Guidelines and Technical Basis section to be included within the standard for clarifications of the following…" ***Who is the vendor? Is it the manufacturer/software company, the reseller the hardware/software is acquired from, the shipping company, the integrator, others? For temporary staff, is the contract employee a vendor?***"

Likes 0	
Dislikes 0	

Response

Bob Case - Black Hills Corporation - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

The intent of FERC Order 829 is noble, but seems to be directed to the wrong audience. The risks of compromised hardware and software impacts much more than ICS, in that it extends to all our processing and communication systems. With the advancement of IoT, the spirit of FERC Order 829 needs to be moved to an even higher national focus. In the meantime, NERC should focus on helping registered entities improve its controls culture within the activity environment it can directly impact. Thanks.

Likes 0	
Dislikes 0	

Response

Devin Elverdi - Colorado Springs Utilities - 1

Answer	
Document Name	

Comment

Refer to CSU comments.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	
Document Name	
Comment	
By not modifying the existing CIP Standards where there is overlap of requirement, there is a distinct possibility of inconsistent policies and procedures. Furthermore, should the Registered Entity choose to reference its other Standards compliance documents, there is a possibility of creating circular references or “spaghetti” linkages.	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	
Document Name	
Comment	
Avista commends the SDT and NERC for the extensive work done on developing this standard. Avista also supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	
Document Name	
Comment	

1) Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

2) This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

3) As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standard.

4) Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

a. Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

b. Move CIP-013 R3, to CIP-010 R1.

c. CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

d. Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	
Response	

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	
Document Name	
Comment	

This Standard implies a high degree of compliance audit and enforcement authority for the Regions, which we have not seen implemented. From our experience with CIPv5 compliance exceptions, the objectives of the Reliability Assurance Initiative to provide risk-based process efficiencies have not been met. Entities must still use the costly self-report process for anything short of perfection, and regional auditors are not given latitude to make risk-based decisions. CIP-013-1 as drafted cannot work as intended until entities can work with regional auditors to quickly assess risk.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5

Answer	
Document Name	

Comment

See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	
Document Name	

Comment

The intent of FERC Order 829 is good, but seems to be directed to the wrong audience. The risks of compromised hardware and software impacts much more than ICS, but extends to all our processing and communication systems. With the advancement of IoT, the spirit of FERC Order 829 needs to be moved to an even higher national focus. In the meantime, NERC should focus on helping registered entities improve its controls culture within the activity environment it can directly impact. Thanks.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	
Document Name	

Comment
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	
Document Name	

Comment
Note of Appreciation We recognize the constraints imposed on the Standard drafting process by the language of the Commission's Order and its directives. We also would highlight Commissioner LaFleur's caution--that the Order was premature—may be coming to fruition. In consideration of both points, we are appreciative of the Standard Drafting Team's continuing work on the CIP Cyber Supply Chain Standard and its efforts to overcome the challenges it presents. Thank you. Kansas City Power and Light Company

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	
Document Name	

Comment
Oxy supports the comments of MRO.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	
Document Name	
Comment	
The current version of CIP-013-1 is vague. Though flexibility is needed, the current version does not provide enough clarification to Registered Entities on the expectations required under the Standard and will therefore fail to mitigate cyber security risks to the BES.	
Likes 0	
Dislikes 0	
Response	

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	
Document Name	
Comment	
We have several questions and concerns about what the phrases "vendor-initiated" and "system-to-system remote access" used in several requirements exactly mean. 1) Can the SDT please clarify what is meant by “vendor-initiated”. For example, if we (the customer) are having an operational issue and contact the vendor for support, is that support session still considered “vendor-initiated”, or would that session not be in scope because it is prompted by the customer’s request? Alternatively, if we initiate the remote access session with the vendor and turn over control to them, is that session still considered "vendor-initiated"? 2) We are unclear what the phrase "system-to-system" means. Please define or give examples of what would be considered a “system-to-system remote access with a vendor”. We are having trouble understanding how we might apply R4.1-4.3 and other associated requirements if there is no human interaction. 3) In our experience, vendor or third-party remote assistance is typically needed in times where there is a problem that could not be resolved by internal staff. We are concerned with the monitoring requirement (4.2), especially in situations where the system issue is having a real-time impact on operations and requires speedy trouble-shooting and resolution. There may not be enough internal resources available to respond to the situation and also actively monitor the vendor’s session. Additionally, the use of the phrase “unauthorized activity” is problematic, as the situation may not allow for a step-by-step explanation from the vendor as to what steps they are taking to troubleshoot the issue. Finally, how would one prove in an audit that the session was monitored and that no unauthorized activity occurred? Tri-State strongly believes the directives issued in Order No. 829 should be addressed by revising existing CIP standards, so that entities have all the relevant requirements together. We are concerned that if the existing standards are not revised to incorporate the new requirements, we will recreate the confusion and complexity that came with v3 standards, which in many cases led to non-compliance. We encourage NERC to request more time from FERC to get this right the first time and to avoid future projects, if extra time is needed, and instead allow the industry to focus more time and resources on getting cyber security right.	
Likes 0	
Dislikes 0	
Response	

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	
Document Name	
Comment	
Concur with EEI’s Position	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	
Document Name	
Comment	
- See APPA's comments.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	
Comment	
NRECA thanks the SDT for its work on this challenging project in such a short amount of time.	
Likes 0	
Dislikes 0	
Response	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	
Document Name	

Comment
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item. EPE looks forward to working collaboratively with NERC staff and stakeholders in clarifying the wording of the various requirements to achieve more effective, efficient and widespread compliance on these important matters.

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	
Document Name	

Comment
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item. EPE looks forward to working collaboratively with NERC staff and stakeholders in clarifying the wording of the various requirements to achieve more effective, efficient and widespread compliance on these important matters.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant

Answer	
Document Name	

Comment
We appreciate the hard work of the standard drafting team in putting together this first draft standard and supporting documents. This is a very different type of standard than usual that asks entities to address risks that may be introduced by activities outside of their control. Although we have concerns with this first draft, we feel confident that the team can work through the issues and come up with a reasonable set of requirements. If low impact Cyber Systems are included in any of the requirements, the requirements should be less stringent than those for high and medium since the risk to the BES is considerably less. Some of the other CIP standards use applicability tables to more clearly illustrate the specific requirements for

each of these impact levels (see CIP-004 for an example). If there are any variations in requirements for the impact levels – especially if low impacts are included in this standard - we would like to see the tables used. They provide consistency with the way the other standards are written, they're easier to navigate, and they can illustrate the risk-based nature of the standard.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item. EPE looks forward to working collaboratively with NERC staff and stakeholders in clarifying the wording of the various requirements to achieve more effective, efficient and widespread compliance on these important matters.	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	
Document Name	
Comment	
Support EEI comments.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	

Document Name	

Comment

The drafting team should consider addressing some sort of vendor certification process to enable entities to select vendors that meet all of the security requirements stated within this standard. This will enable entities to rely on these vendors while allowing the entity to expeditiously address security vulnerabilities and other risks to operations.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

At the outset, Southern Company wishes to first note for the record its belief that Requirement R3 and Requirement R4 should be removed from the CIP-013 standard. As explained below, it is either duplicative of R1, duplicative of existing requirements in CIP-004-6, CIP-005-5, CIP-007-6, CIP-008-5, and CIP-010-2, and is inappropriate for a standard focused on the Supply Chain time horizon.

First, from the perspective of a supply chain procurement time horizon, verification of the integrity and authenticity of software and firmware is already addressed under Requirement R1, R1.2.3. Specifically, R1 requires a risk management plan that addresses controls for mitigating cybersecurity risks for industrial control system vendor products and services, and the plan must address methods to evaluate controls to address those risks (R 1.2) including “process(es) for verifying software integrity and authenticity of all software and patches that are intended for use”. (R 1.2.3) Specifically, (assuming R1 covers only the procurement time horizon), then R3’s requirement -- to implement “one or more documented processes” to address the verification of the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems -- is arguably covered by R1.2.3’s requirement to have a process to do the same with respect to all industrial control system software and patches.

Second, to the extent R1 or R3 could be read to extend to verification of authenticity/integrity beyond the procurement and into the operational phase, such a broad interpretation should be outside of the scope of the CIP-013 supply chain standard, and would be more appropriately addressed in a separate proceeding to look specifically at operational standards CIP-002 through CIP-010. Specifically, patch monitoring and management is already described in CIP-007, yet little consideration appears to have been given to the burdensome impacts that might result on CIP-007 compliance if CIP-013 R3 compliance is layered on top in the operational time horizon, rather than being limited to the procurement phase (and thus covered in CIP-013 R1). The stringent 35 day cycles required within CIP-007-6 R2 will be significantly impacted by the proposed language in R3, placing Responsible Entities in a position of compromising compliance with one standard by trying to maintain compliance with another. The supply chain NOPR and final were not originally focused on these types of operational controls, and any such exploration of operational risk issues are more appropriately explored separately and outside of the supply chain proceeding. Moreover, if this standard is intended to cover all aspects of all lifecycle stages (from planning to procurement to production to retirement, i.e., cradle to grave) for all devices and vendors – that is an expansive initiative that overlaps with multiple CIP standards and would require a timeframe for development that is much longer than one year.

Similarly and for the above reasons, Requirement R4 is also considered not necessary and should be removed. The proposed requirement for "authorization of vendor remote access" is already explicitly required in CIP-004-6 R4; logging and monitoring of vendor remote access is already covered in CIP-005-5 R1 and CIP-007-6 R4; and response to "unauthorized activity" by vendors is already covered in CIP-008-5. The modifications provided above and suggested under R4 are to address the Responsible Entity having the capability to quickly disable vendor remote access sessions, which again we strongly recommend the SDT consider incorporating into CIP-005 as a new requirement addressing this potential security improvement.

Overall, industry was not given an adequate chance to express this in the FERC proceeding leading to Order 829 because the NOPR expressed proposed directives at a very broad and high level whereas the Final Rule contained much more prescriptive directives. Southern Company agrees with the July 21, 2016 statement provided by Acting Chairman LaFleur in this proceeding that "the more prudent course of action" for NERC, industry, and stakeholders would have been to issue a supplemental NOPR to provide input on the more prescriptive directives contained in this Final Rule. Southern Company would encourage an opportunity for input on such larger matters once the standard is submitted to the Commission for approval. Having said that, Southern Company recognizes and appreciates that, at this stage of standard development, NERC is bound to comply with the final rule's directives in Order 829. Therefore, while wishing to preserve for the record its opinion that Requirement R3 and R4 should be removed, Southern Company offers the comments and language contained herein to improve the standard from its currently drafted version.

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	
Document Name	

Comment

ITC agrees with the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	Project 2016_03_ Exelon Comments_ 030617.docx
Comment	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-03 Cyber Security Supply Chain Risk Management

DO NOT use this form for submitting comments. Use the electronic form to submit comments on proposed **CIP-013-1 – Cyber Security - Supply Chain Risk Management**. The electronic comment form must be completed by **8:00 p.m. Eastern, Monday, March 6, 2017**.

Documents and information about this project are available on the project page. If you have any questions, contact Standards Developer, Mark Olson (via email), or at (404) 446-9760.

Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829 directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> "[The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

NERC must file the new or revised Standard by September 27, 2017, to meet the one-year deadline established by the Commission in Order No. 829.

The standard drafting team (SDT) has developed proposed CIP-013-1 to address the above directives.

Questions

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you

agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No

Comments:
The draft Requirement R1.2 language creates compliance concerns due to the need for Responsible Entities to negotiate commercial contracts with vendors that commit the vendors to undertake the tasks necessary for R1.2, particularly in circumstances where only a single vendor has the capability of providing the necessary services for Cyber Assets covered by CIP-013-1. For example, unless a vendor agrees to notify the Responsible Entity of vendor-identified vulnerabilities in the Cyber Assets provided or maintained by the vendor, Responsible Entities cannot comply with R1.2.3.

Responsible Entities could encounter scenarios where:

- Vendors may refuse to comply with the Responsible Entity's vendor controls;
- Vendors may demand an unreasonably high payment for compliance with the Responsible Entity's vendor controls;
- Vendors may agree to Responsible Entity controls but fail to take the steps necessary to implement those controls in a compliant manner; or
- Software/firmware made by a vendor no longer in business and unable to assist the Responsible Entity in the integrity and authenticity verification process.

To ensure that compliance with CIP-013-1 does not place Responsible Entities in an untenable negotiating position, a compliance "safety valve" is necessary to allow Responsible Entities to comply with the Standard even in the absence of vendor assent to the Responsible Entity's required controls. Such a "safety valve" would be consistent with the current draft guidance on CIP-013-1 R1.2, which states that "[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Guidance language in the G&TB portion of a Standard is helpful, but the "safety valve" concept should be included within the language of the Requirement itself because only that language forms the basis of a compliance assessment.

Exelon has sent ideas under separate cover to the Drafting Team Chair outlining three options for providing the necessary "safety valve" along with proposed text edits to the requirements. In short, these options include a technical feasibility exception, a commercial feasibility exception or a simple exception documentation process.

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply

chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Exelon feels that the R2.1 language is vague and has the potential to become administratively burdensome without a corresponding benefit to BES reliability. While Exelon agrees with the rationale that examples of sources of information that an entity could consider include guidance or information issued by the E-ISAC, this language should be included in the Requirement itself because only that language forms the basis of a compliance assessment. Exelon receives over 100 security-related messages regarding potential vulnerabilities per day from a myriad of sources. Without creating bounds around the sources to be considered as well as the periodicity for updates to supply chain cyber security risk management plan(s), the question of whether any or all of the messages should have been considered will be difficult, if not impossible, to evidence. Exelon points out that the E-ISAC already performs important filtering functions for the industry. Perhaps future Alerts issued by the E-ISAC could be enhanced to point out vulnerabilities that would require new mitigating controls in supply chain cyber security risk management plan(s). Without these limitations, each entity will need to develop processes and procedures to receive and filter information, define mitigating controls, update the plan(s) and obtain approvals which is inefficient at best and impossible to evidence at worst.

Further, Exelon suggests that while multiple updates to the plan(s) may occur within a year as new E-ISAC Alerts are issued, CIP Senior Manager Review and Approval should only be required every 15 months. Intermediate reviews and approvals, or reviews for minor changes, should be outside the scope of the Requirement.

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

The draft Requirement R3 language creates compliance concerns due to the need for Responsible Entities to negotiate commercial contracts with vendors that commit the vendors to undertake the tasks necessary for R3 compliance, particularly in circumstances where only a single vendor has the capability of

providing the necessary services for Cyber Assets covered by CIP-013-1. For example, unless the vendor agrees to cooperate with any software integrity and authenticity verification process, the Responsible Entity will be unable to ensure the integrity and authenticity of software used in covered Cyber Assets.

Responsible Entities could encounter scenarios where:

- Vendors may refuse to comply with the Responsible Entity's vendor controls;
- Vendors may demand an unreasonably high payment for compliance with the Responsible Entity's vendor controls;
- Vendors may agree to Responsible Entity controls but fail to take the steps necessary to implement those controls in a compliant manner; or
- Software/firmware made by a vendor no longer in business and unable to assist the Responsible Entity in the integrity and authenticity verification process.

To ensure that compliance with CIP-013-1 does not place Responsible Entities in an untenable negotiating position, a compliance "safety valve" is necessary to allow Responsible Entities to comply with the Standard even in the absence of vendor assent to the Responsible Entity's required controls. Such a "safety valve" would be consistent with the current draft guidance on CIP-013-1 R1.2, which states that "[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Guidance language in the G&TB portion of a Standard is helpful, but the "safety valve" concept should be included within the language of the Requirement itself because only that language forms the basis of a compliance assessment.

Exelon has sent ideas under separate cover to the Drafting Team Chair outlining three options for providing the necessary "safety valve" along with proposed text edits to the requirements. In short, these options include a technical feasibility exception, a commercial feasibility exception or a simple exception documentation process.

Exelon does not support the draft language in R3 which requires an Entity to verify the integrity and authenticity before placing a BES Cyber System into operation. Instead, Exelon prefers the suggested language from Order No. 829 that directs "the integrity of the software and patches before they are installed in the BES Cyber System environment" (P. 48). Accordingly, Exelon suggests that R3 be edited to read as follows:

Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware **prior to installation into** high and medium impact BES Cyber Systems

In addition, see the concerns under (4) below regarding potential overlap between R3 and existing CIP Standards.

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

The proposed Requirement creates significant overlap with existing CIP Requirements. Requirement R4, as well as Requirements R3 and R5, should be modified so that CIP-013 only addresses those aspects of software integrity and authenticity (R3), remote access (R4), and authenticity and remote access for low impact BES Cyber Systems (R5) not covered by other Standards. Exelon understands that the timeframe dictated by FERC in Order No. 829 does not allow for revisions by this SDT to the relevant Standards that address these topics. However, overlap between the Standards should be avoided as much as possible to avoid double jeopardy concerns in the event of potential non-compliance with CIP-013 R3, R4, and R5.

For example, Exelon's review of the draft CIP-013-1 Standard indicates the following areas of overlap:

- CIP-013-1 R3.1 through R3.4 require authentication of operating systems, firmware, software, and patches. However, the configuration change management requirements under CIP-010-2 R1 already require that the configuration of operating systems, firmware, and software be carefully tracked such that counterfeit operating systems, firmware, software, and patches would be identified (e.g. a software difference would be identified as a change from the existing baseline configuration) and would be evaluated.
- CIP-013-1 R3.4 requires authentication of patches, updates, and upgrades, but CIP-007-6 R2.1 already imposes a patch management process for tracking, evaluating, and installing cyber security patches, including the identification of patching sources. Part of the identification of patching sources under CIP-007-6 is the verification that those sources are authentic as CIP-013-1 R3.4 would appear to require.
- CIP-013-1 R4.1 requires authorization of remote access to certain BES Cyber Systems by the vendor. CIP-004-5 R4.1.1 already contains a process for authorizing electronic access to these assets by all personnel, including vendors.
- CIP-013-1 R4.2 requires logging and monitoring or remote access sessions. CIP-007-6 R4.1 already requires logging of all access and CIP-007-6 R4.2 requires alerting for any malicious code as well as any "security ecent that the Responsible Entity determines necessitates an alert."
- CIP-013-1 R4.3 also requires responding to detected unauthorized activity, and because unauthorized activity on a BES Cyber System would constitute a "Cyber Security Incident," CIP-008-5 already requires a response to such incidents.

- CIP-013-1 R5 requires a process for controlling vendor remote access to low impact BES Cyber Systems. This overlaps with CIP-003-6 Attachment 1 Section 3 which already requires electronic access controls for low impact BES Cyber Systems the limit access to necessary access.

The draft CIP-013-1 requirements should be modified so that overlaps are removed and that CIP-013-1 only addresses vendor issues not covered within existing Standards. To the extent the SDT believes there is no overlap between CIP-013 and the existing CIP Standards, the SDT should explain in each instance where the CIP-013 Requirement ends and the other CIP Requirement begins. In the absence of such guidance, a Compliance Monitoring and Enforcement Process could conclude that a particular instance of non-compliance with CIP-013 is also a simultaneous violation of another Reliability Standard, doubling the available penalty range. For example, draft CIP-013-1 R4 requires the Responsible Entity to authorize remote access by vendor personnel. The current CIP-004-6 R4.1.1 also requires authorization of vendor personnel to have electronic access. Therefore noncompliance with CIP-013-1 R4 would appear to, per se, constitute noncompliance with CIP-004-6 R4.1.1. Such double jeopardy serves no apparent reliability purpose. If the current CIP-013-1 R4 language is adopted as-is, the SDT should explain how its requirements differ from those under CIP-004-6 R4.1.1.

Finally, Exelon suggests that R4.3 may be difficult to accomplish in all cases and is overly prescriptive and thus should be removed from CIP-013. Order No. 829, P.52 references the Ukraine event and the threat that "vendor credentials could be stolen and used to access a BES Cyber System without the responsible entity's knowledge, as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a responsible entity's BES Cyber System." There are alternate methods to address this threat. First, two factor identification methods can be used to mitigate the risk of stolen credentials. Second, the use of WebEx or Skype sessions or active control of vendor access (i.e. opening a port for access only when needed) can be used to address emergent issues and reduce the need for remote persistent sessions.

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Exelon has the same concerns regarding the lack of a compliance "safety valve", the potential for double jeopardy as well as the administrative burden of updating the supply chain cyber security risk management plan(s) for newly identified vulnerabilities as included in the comments on R1-R4. The discussion under (4) identifies how the proposed R5 overlaps with existing CIP Standards.

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

☒ Yes
☐ No
Comments:

Exelon generally agrees with the Implementation Plan for CIP-013-1 but offers the following recommendation for clarifying the plan for R2.

The initial review and update, as necessary, of cyber security risk management plans specified in Requirement R2 must be completed within fifteen (15) calendar months **following** the effective date of CIP-013-1. There should be no obligation to review the plans ahead of time, and only the initial development and implementation should be required. This should be made clear in the Implementation Plan.

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

☐ Yes
☒ No
Comments:

On Page 9, line 43, the Technical Guidance and Examples references the use of industry best practices and guidance that improve cyber security risk management controls. This does not match the rationale of R2 which only speaks to the use of guidance. Exelon feels that the reference to "industry best practices" should be removed from the Technical Guidance and Examples since it is non-specific and open to interpretation.

9. Provide any additional comments for the SDT to consider, if desired.

Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-03 Cyber Security Supply Chain Risk Management

DO NOT use this form for submitting comments. Use the electronic form to submit comments on proposed **CIP-013-1 – Cyber Security - Supply Chain Risk Management**. The electronic comment form must be completed by **8:00 p.m. Eastern, Monday, March 6, 2017**.

Documents and information about this project are available on the project page. If you have any questions, contact Standards Developer, Mark Olson (via email), or at (404) 446-9760.

Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829 directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> "[The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

NERC must file the new or revised Standard by September 27, 2017, to meet the one-year deadline established by the Commission in Order No. 829.

The standard drafting team (SDT) has developed proposed CIP-013-1 to address the above directives.

Questions

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you

agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

ERCOT supports the IRC comments and offers the following supplemental comments.

FERC Order 829, Paragraph 59, states that NERC's new or modified standard "must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations." This does not include the Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs) listed in R1. These systems do not perform or provide bulk electric system operations. ERCOT believes the inclusion of these systems in the draft standard goes beyond the scope of the standard intended by FERC and recommends the SDT remove them from the applicable systems of the standard language.

Requirement R1 requires Responsible Entities to have a plan that addresses processes for notification of a vendor's cyber security events (R1.2.1) and vulnerabilities (R1.2.3), as well as coordination of cyber security incident response activities (R1.2.4). As this information is highly sensitive, it is unlikely that all vendors will agree in all cases to provide this information unless they are already required to do so under other regulatory obligations. Responsible Entities cannot force a vendor to agree to these terms, and in cases where the vendor deems the risk of this disclosure too great compared to the value of the contract, the vendor will decline to enter into the agreement. This will force the Responsible Entity to seek another vendor that is willing to accept these terms, and such a vendor may or may not exist. Because it is possible that a Responsible Entity may be unable to identify a vendor that is willing to accept a contract with the terms required by R1, the proposed standard could seriously hamper the essential functions of Responsible Entities. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R1. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

Requirement R1.2.2 requires "notification when vendor employee remote or onsite access should no longer be granted." The revocation of access, including Interactive Remote Access, is currently addressed in CIP-004, R5. Since the background checks, training, access authorization, and access revocation for employees and vendors is already addressed in CIP-004, the drafting team should ensure any new requirements related to access revocation of vendors be placed in CIP-004. In developing the CIP Version 5 standards, extensive work was undertaken to ensure that all requirements related to the subject were included in one standard instead of being spread across multiple standards. The proposed language will disrupt that framework.

Requirement R1.2.5, which requires a Responsible Entity's plan to include "Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use," is duplicative of Requirements R3 and R5 within this standard, which also require documentation of processes. ERCOT recommends removing R1.2.5.

Requirement R1.2.6 requires an entity's plan to include "Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)." This requirement is duplicative of Requirement 4 within this standard. ERCOT recommends removing Requirement R1.2.6, which also requires documentation of processes.

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☒ Yes
☐ No
Comments: ERCOT supports the IRC comments on this question.

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

ERCOT supports the IRC comments on this question and offers the following supplemental comments.

ERCOT recognizes the need for the concepts contained in Requirement R3. However, ERCOT disagrees with the placement of the requirement in a new standard. Since this requirement is applicable to only high and medium impact BES Cyber Systems, it should be placed within CIP-010. The requirement directly impacts the baselines that have been established within CIP-010 R1. The SDT could insert a new part between existing Parts 1.1 and 1.2 in that standard. The new part could use the following language: "For any updates or patches that that deviate from the existing baseline configuration, verify the authenticity and integrity of the update or patch." As mentioned previously, in developing the CIP Version 5 standards, the SDT performed extensive work to ensure that all requirements related to a particular subject were included in one standard instead of being spread across multiple standards. The proposed language will

disrupt that framework. Including the requirement in CIP-010 will ensure that a single standard captures all parts of the change process, including inventory (Part 1.1), validation of the code (NEW), authorization of implementation (Part 1.2), update of the inventory (Part 1.3), and testing of the change (Parts 1.4 and 1.5). This approach would give Responsible Entities a complete view of what is required from the start to the end of a change. It also prevents entities from keeping separate inventories to meet the CIP-010 requirement and the CIP-013 requirement.

Additionally, ERCOT requests guidance on how to demonstrate compliance when using automated solutions to obtain the most current patches applicable to their systems. In large environments, these automated solutions are critical to meeting the timing obligations of CIP-007 R2. Inserting the manual step of verifying integrity and authenticity of updates and patches can prevent the use of these solutions that entities have invested in and rely upon for addressing security risks and regulatory obligations. If it is intended that the entity may simply document the source used by these solutions, it would be helpful to put such clarifying language in the requirement.

Additional use cases for the SDT to consider in developing guidance include: (1) how signature and pattern updates are contemplated within the requirement since these are not updates to the operating system, software, or firmware noted, (2) instances when code is packaged and mailed to an entity, (3) software and firmware that are part of a vendor black-box type of appliance solution where the entity has no visibility to the code on the device, and (4) vendors bringing code onsite that the entity is not allowed to review. Any of these cases could present an obstacle to strict compliance with the draft standard language.

As with Requirement R1, this requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. The drafting team should address situations in which vendors will not or cannot provided the levels of service mandated by this requirement. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R3. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

ERCOT supports the IRC comments and offers the following supplemental comments.

Requirement R4 is duplicative of existing requirements in CIP-004, CIP-005, CIP-007, and CIP-008. The drafting team should consider modifications to these existing standards rather than creating new requirements in a new standard. By placing these requirements in a stand-alone Standard, there is a possibility that entities may not make necessary connections to the prerequisites of some requirements (e.g., CIP-004 R2, R3) and downstream obligations of other requirements (e.g., CIP-008). ERCOT offers the following suggestions for realignment:

Requirements for electronic access authorization of vendors, including Interactive Remote Access, are addressed within CIP-004 R4, which also addresses the proper vetting and training of said vendors. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper pre-authorization requirements.

Requirements for Interactive Remote Access are already addressed within CIP-005 R2. Vendor-initiated remote access is just one example of Interactive Remote Access. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper configuration of remote access (e.g. multi-factor authentication, encryption, Intermediate System).

Requirements for system-to-system communications are already addressed within CIP-005 R1. This requirement could be added to CIP-005 R1 or as an addition to R2. The heading for Table 2 within CIP-005 can be modified to “Remote Access” in support of this. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper network controls for the system-to-system communication (e.g. ESPs, EAPs, etc.).

Requirements for logging and monitoring of access activity are addressed in CIP-007 R4. If the SDT keeps the requirement in CIP-013, the requirement should be modified to identify the logging specifications that differ from CIP-007 R4.

Requirements for response to unauthorized activity are already addressed within CIP-008. If the SDT keeps the requirement in CIP-013, the requirement should be modified to identify integration with CIP-008.

There are also several instances in the standard where language needs to be clarified. The drafting team should state whether system-to-system remote access includes “phone home” capabilities that are used for reporting of licensing, system health, and system problems. Requirement R4.1 should be clarified to specify whether it is addressing authorization of each remote access session or remote access to the vendor in whole. The drafting team should consider whether this requirement is consistent with current requirements in CIP-004 R4. The drafting team also needs to address authorization of software companies that use a “follow-the-sun” support model. Follow-the-sun is a type of global support where

issues are passed around daily between work sites that are many time zones apart. Such a support increases responsiveness.

As noted with other requirements in the draft CIP-013 standard, the drafting team should address situations in which vendors will not or cannot provide the levels of service mandated by this requirement. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling to agree. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R4. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

As with other comments, this requirement is duplicative and should be placed within the security plan under CIP-003 Attachment 1 for low impact BES Cyber Systems. Current standards have been drafted to allow entities with low impact BES Cyber Systems to refer to a single standard to for security plan requirements.

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Twelve months is not sufficient time to allow compliance with all aspects of this standard. The drafting team should consider a phased approach allowing the logical phased implementation of these requirements.

While the Implementation Plan suggests that existing contracts need not be modified, the proposed standard language does not make this clear. ERCOT believes the standard to be a more appropriate

location for this exemption, as it is ultimately substantive in nature. ERCOT there recommends that the drafting team include language in the standard explicitly limiting applicability of the requirements to new contracts.

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

☒ Yes
☐ No
Comments: No comments

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

☐ Yes
☒ No
Comments:

Although NERC's Compliance Guidance Policy document describes certain procedures by which a drafting team may provide Compliance Guidance, ERCOT suggests that it is generally preferable to provide examples of acceptable conduct in the standard itself, rather than in an ancillary document, which Responsible Entities would have to remember and separately locate and review. The team could achieve this purpose by using language in the standard such as: "Practices that comply with this requirement include, without limitation, the following: . . . ." ERCOT notes that in a number of instances, the draft Technical Guidance and Examples document uses normative language (e.g., "should"), rather than permissive (e.g., "may") language, which suggests that the Technical Guidance document is instead intended to serve simply as a more detailed set of requirements, as opposed to describing one of potentially many acceptable methods of achieving compliance. For example, the guidance for R1 states: "In implementing Requirement R1, the responsible entity should consider the following: . . . ." To the extent the drafting team intends the guidance in this document to be followed, it should be included in the standard.

9. Provide any additional comments for the SDT to consider, if desired.
Comments:
The drafting team should consider addressing some sort of vendor certification process to enable entities to select vendors that meet all of the security requirements stated within this standard. This will enable entities to rely on these vendors while allowing the entity to expeditiously address security vulnerabilities and other risks to operations.

Foundation for Resilient Societies Comments on Draft Standard 2016-03, Cyber Security Supply Chain Risk Management, NERC CIP 013-01

1. Vote "NO" on approval of the draft.

   Rationale: The proposed CIP-013-01 standard is onerous and not cost-effective. It excpectss too much of individual registered entities, which should not be the primary organizations responsible for strengthening the integrity of the cyber supply chain.

   Starting at the foundry level, it is essential to assure the integrity of chip design, manufacture and operations. And control of firmware by entities that are committed to protect the national security interests of the United States and Canada. The current practice of purchasing control and telecommunication systems from the lowest-cost supplier may be too risky and too imprudent to attain greater integrity in cyber supply chains. It is unreasonable to expect that some 1400 separate electric utilities should be responsible for major changes in the development and regulation of cyber supply chain systems.

   The recent re;port on Cyber Deterrence by the Defense Science Board, released on February 28, 2017, seeks tailored initiatives to enhance deterrence of cyber attacks on critical infrastructures. This Report recognizes that a key element of deterrence is to improve defenses, so the payoffs to foreign adversaries will be reduced. Meanwhile, the Trump Administration has underway a review of cyber policies and strategy. If the Administration will support initiatives to strengthen cyber supply chains that involve indigenous U.S. design, production, operation, and integrity testing for the entire cyber supply chain, any final NERC-FERC standard responsive to Order No. 829 should await opportunities to be presented by the Administration after its policy review.

   As a result of this overburden on registered entities, the Standard Drafting team -- not surprisingly -- has drafted CIP-013-1 containing too many exceptions, qualifications, and outstanding conflicts to form the foundation for the most-difficult process of managing the risks that derive from vulnerabilities in products marketed to the industry in a global and highly competitive environment. If some foreign governments subsidize their hardware systems, is it imprudent to always accept the lowest price products that place our cyber supply chains at risk?

   The present draft standard makes the probability of successful discrimination exceedingly low. The investment of time and money by utilities and the industry will be very high, and certainly not worth the risks of failing compliance by entities and their procurement selections that are even further removed from technical competencies essential to their task.

   Implementation as written will only encourage a shell game that will delay real solutions to the Supply Chain vulnerabilities and provide false assurances that must be addressed collectively by the industry, by state and by federal authorities. The latter must address the increasing failures of vendors to design secure products through market motivations and penalties. This problem has been successfully addressed in many other industries where serious safety issues existed.

2. **Requirement R1**
   a. Any deep examination of the four objectives of R1 reveals substantial gulfs with the realities of Supply Chain issues.

- Risks can never be assessed in the absence of vulnerability assessments. None are called for. And vulnerabilities range from individual components to full systems. End-to-end control center to remote unit network assessments are needed.
- A component flaw might trace to a vendor several stages removed from the utility and vulnerabilities are often the product of several vendors' missteps.
- Adversarial efforts impact multiple systems and subsystems; hardware and software and firmware, classical attack vectors and subtleties difficult for even professional forensic experts. These challenges are beyond utilities' ability to assess.
- The "prior contract" exclusion leaves open vulnerabilities introduced post "contracting." Note that the February 2017 Defense Science Board Report on Cyber Deterrence calls for improvements in defensive capabilities as a key element of deterrence. The "prior contract" exception will assure access by foreign adversaries that will enable continuing implantation of malware, continuing exercise of equipment within the U.S. electric grid and within other critical infrastructures upon which the North American electgric grid depends. . These"prior contract" exceptions are inexcusable; a program needs to be developed -- not by individual registered entities -- to assist in the removal and replacement of hazardous hardware, firmware, and software.
- The absence of hard requirements for "secure vendor accesses", "Internet avoidance", "encryption", "blacklisting known malware", etc. reveals industry ambivalence re: enforceable supply chain controls.
- No plan can possibly be developed that will adequately cover the variety of situations and conditions that exist. They are far too complex to be "planned for" separately by over 1400 independent "Responsible Entities". And we observe the usual escape clause, ***"Obtaining specific controls in the negotiated contract may not be feasible and it is not considered failure to implement an entity's plan".*** How does one define ***success***, under these circumstances?

b. **Requirement R2**. The R2 process is clearly a bureaucratic device; an artificial deadline for updating the plan, get approval from the senior CIP manager (who should have sustained involvement, not at 15 month intervals.) If this process is adopted and approved, the net result will be to undermine the goal of cyber deterrence as enunciated in the February 2017 Defense Science Board Report. Intervals of 15 months between assessments and corrections will enable large gaps that foreign adversaries will exploit.

c. **Requirement R3.** Implementing one or more documented processes for verifying the integrity and authenticity (medium and high impact BES systems) for software and firmware would require substantial forensic competency by the utility. Further, in the reality of the sophisticated attacks that have given rise to Order No. 829, there is very little likelihood of success by over 1400 independent "responsible entities" and the potential for unreasonable expenses in the process. Or did the SDT intend to minimize

the task? This illusory requirement illustrates the need for broader initiatives, both within the electric utility industry and outside the industry.

d. **Requirement R4.** The requirement for controlling vendor remote access seriously ignores many gaps and related problems In CIP v5/v6, in the categorization structure and in the process proposed. It fails to lay down hard controls on vendor access and yet requires a complex "documented" process which can easily pass table top compliance review without correcting the many holes in systems as they operate that will remain available to adversaries. Exceptions to CIP standards leave thousands of cyber assets directly interfacing with the internet, not covered by this standard as well as all others. Yet those assets are directly linked to OT and IT systems providing paths for malware, data corruption and opportunities for adversarial control, through supply chain vulnerabilities. With respect to Supply Chain vulnerabilities, Grid connectivity makes nonsense of the categorization of Cyber Assets as "low", "medium" and "high" impact.

e. The practice of rating a low impact asset as "no effect on the BES overall" has consistently ignored the sum of such assets effect on the vulnerabilities of the Grid to uncontrled separation and cascading outages, and permanent damage to long-replacement-time grid equipment.

f. **Requirement R5**. Given the holes described in **R4**, this requirement for verifying product integrity and controlling vendor accesses, and presumably unmonitored machine-to-machine accesses for the few low impact cyber assets covered by CIP standards, is intended to obscure the realities of major portals available to the nation's adversaries. FERC knows CIP standards utterly fail to address the vulnerabilities of so-called low level , so-called "Low Impact" cyber assets, as have been demonstrated to enable takedown of elements of the Ukrainian electric distribution system in both December 2015 and December 2016 . FERC knows that such assets represent major avenues for attack on the BES and the short path to "Distribution" systems and nuclear sites. Notwithstanding, the current supply chain standard needs a major overhaul to provide effective and verifiable system security.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-03 Cyber Security Supply Chain Management

DO NOT use this form for submitting comments. Use the electronic form to submit comments on proposed **CIP-013-1 – Cyber Security - Supply Chain Risk Management**. The electronic comment form must be completed by **8:00 p.m. Eastern, Monday, March 6, 2017**.

Documents and information about this project are available on the project page. If you have any questions, contact Standards Developer, Mark Olson (via email), or at (404) 446-9760.

Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829 directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> "[The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

NERC must file the new or revised Standard by September 27, 2017, to meet the one-year deadline established by the Commission in Order No. 829.

The standard drafting team (SDT) has developed proposed CIP-013-1 to address the above directives.

Questions

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you

agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:
Seattle City Light has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

Seattle City Light does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, Seattle City Light requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, Seattle City Light believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, Seattle City Light requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

Seattle City Light requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

Seattle City Light is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as national, regional, state & city negotiated contracts. Examples include contracts from the National Association of State Procurement Officials (NASPO) Cooperative and the Western States Contracting Alliance. In some cases use of these contracts in procurement is mandated by other laws or regulations. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they provide important negotiating strength, flexibility, and effectiveness in contracting (see Seattle City Light’s response to Question #9 for additional information on exceptions).

Seattle City Light notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 Seattle City Light requests changing the word *evaluate* to *determine.*

For R1.2.1 Seattle City Light requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 Seattle City Light requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. Seattle City Light requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

In Measure M1, Seattle City Light requests that the language be changed to be consistent with the Requirement. Specifically, change "Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…" to "Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…" (BOLD emphasis added). The construction "address risk" conforms with the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as alternatives to being mitigated.

Seattle City Light requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☒ Yes
☐ No
Comments:

Seattle City Light agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, Seattle City Light requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s)

specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Seattle City Light requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Seattle City Light requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. Seattle City Light requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Seattle City Light requests changing the language to “upon detected unauthorized activity”.

Furthermore, because it may not be technically feasible to remotely disable a vendor from equipment provided by that vendor (which the entity purchased from them, and may be dependent upon the vendor for maintenance), Seattle City Light requests the inclusion of a Technical Feasibility Exception (TFE) for R4. Seattle City Light suggests the following language: "WHERE TECHNICALLY FEASIBLE, each responsible entity shall implement one or more documented process(es) for controlling vendor remote access to…" (emphasis added).

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Seattle City Light is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. Seattle City Light requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, Seattle City Light requests that all requirements related to low impact assets be included in CIP-003.

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Seattle City Light does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. Seattle City Light requests a 24-month implementation plan.

Seattle City Light requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Seattle City Light does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Seattle City Light requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Seattle City Light requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

☐ Yes
☒ No
Comments:

Seattle City Light requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging.

Seattle City Light requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

Seattle City Light requests clarification on the term "supplier" as it is used in the guidance document. Seattle City Light requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, Seattle City Light requests an explanation on how the term "vendor" used in the requirements relates to "supplier's system component, system integrators, or external service providers."

The Rationale sections of CIP-013 standard and the guidance document use the term "information system". Seattle City Light requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced Seattle City Light requests that the SDT define the term and place it in the NERC Glossary of Terms.

Seattle City Light requests that the SDT consider defining the term "Security Event" (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. Seattle City Light requests that the following language added to the definition "have potential adverse impacts to the availability or reliability of BES Cyber Systems" and that the entities be required to report only newly identified security vulnerabilities.

Additionally, Seattle City Light requests that the SDT define the term "vendor security event" or replace it with "identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System."

9. Provide any additional comments for the SDT to consider, if desired.
Comments:

Seattle City Light understands that the SDT is under time constraints in addressing Order No. 829, however, Seattle City Light requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

Seattle City Light requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

Seattle City Light feels that all standards with requirements that apply to low impact assets should be included in CIP-003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to Seattle City Light if this was intentional for R3 and R4. Seattle City Light requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

As discussed in comments to R1 above, Seattle City Light requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk.

Seattle City Light recognizes the importance of regulatory bodies and the regulatory industry jointly addressing issues concerning cybersecurity and the reliability of the bulk electric system. In this standard, City Light agrees with other industry comments that many of the gaps addressed in CIP-013 should be modified in other standards and not established as a new standard nearly duplicative of (or worse, in conflict with) other standards. FERC provided NERC the opportunity to either develop a new or modified standard, and City Light urges the SDT to pursue the latter option as much as is appropriate. Requirements in CIP-013 to address the gaps that remain must be carefully crafted to avoid creating an ineffective, unauditable and unenforceable standard. Additionally, the short timeframe for submission of this standard and implementation period restricts the utility industry from contributing meaningful and thoughtful comments that would better focus on supply chain concerns. Thus this standard "does not advance the security of the grid," as set out by now-Chairperson LaFleur in her dissent to Order 829.