NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2016-03 Cyber Security Supply Chain Risk Management | CIP-005-6, CIP-010-3, CIP-013-1
Comment Period Start Date:	5/2/2017
Comment Period End Date:	6/15/2017
Associated Ballots:	2016-03 Cyber Security Supply Chain Risk Management CIP-005-6 IN 1 ST 2016-03 Cyber Security Supply Chain Risk Management CIP-010-3 IN 1 ST 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 AB 2 ST

There were 101 sets of responses, including comments from approximately 220 different people from approximately 141 companies representing 10 of the Industry Segments as shown in the table on the following pages.

The Project 2016-03 Standards Drafting Team (SDT) appreciates the careful review and constructive feedback from stakeholders. The SDT made clarifying and non-substantive changes suggested by stakeholders to the proposed Reliability Standards as follows:

CIP-013-1

- Clarified wording in Requirement R1 Part 1.2.4 for consistency
- Revised examples of procurement processes listed in Requirement R1 rationale to include cooperative purchase agreements
- Clarified in Requirement R3 rationale that responsible entities are not required to renegotiate contracts when implementing updated plans
- Revised the Violation Severity Level (VSL) for Requirement R2 to describe four levels (Lower, Moderate, High, and Severe)

CIP-005-6

- Revised rationale to clarify that responsible entities do not need to implement remote access management processes if they do not allow remote access to applicable BES Cyber Systems, consistent with approved CIP-005-5
- Clarified in the rationale that the phrase *vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* used in the Requirement covers all remote access sessions with vendors.
- Revised VSL for Requirement R2 to include an additional level (High)

CIP-010-3

- Clarified in Requirement R1 Part 1.6 that responsible entities are required to perform software verifications **prior to** a change in baseline
- Revised the Measure for Part 1.6 to include evidence that could apply to automated update systems
- Added information to the Guidelines and Technical Basis section for Requirement R1

Implementation Plan

- Revised examples of procurement processes listed in General Considerations to include cooperative purchase agreements
- Adopted clearer wording for General Considerations section as recommended by commenters
- Added statement to affirm applicability to high and medium impact BES Cyber Systems only
- Included implementation provisions for planned and unplanned changes in categorization consistent with Version 5 CIP Standards implementation

Responses to all comments are provided in the following sections.
All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Director of Standards Development, Steve Noess (via email) or at (404) 446-9691.

Questions

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the 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. The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 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). The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT's removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

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

The Industry Segments are:

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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	1,3,4,5,6	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Southern Company - Southern Company Services, Inc.	Brandon Cain	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Alabama Power Company	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					William D. Shultz	Southern Company - Southern Company Generation	5	SERC
					Jennifer Sykes	Southern Company - Southern Company Generation and Energy Marketing	6	SERC
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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
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
SRC	David Francis	1,2	FRCC,MRO,NPCC, RF,SERC,SPP RE,Texas RE,WECC	SRC + SWG	Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Terry BIlke	Midcontinent ISO, Inc.	2	RF
					Elizabeth Axson	Electric Reliability Council of Texas, Inc.	2,3	Texas RE
					Ben Li	IESO	1	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC
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
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
Associated Electric	Mark Riley	1		AECI & Member G&Ts	Mark Riley	Associated Electric Cooperative, Inc.	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Cooperative, Inc.					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC
					Todd Bennett	Associated Electric Cooperative, Inc.	3	SERC
					Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					William Price	M and A Electric Power Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
	Michael Shaw	6			Teresa Cantwell	LCRA	1	Texas RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Lower Colorado River Authority				LCRA Compliance	Dixie Wells	LCRA	5	Texas RE
					Michael Shaw	LCRA	6	Texas RE
BC Hydro and Power Authority	Patricia Robertson	1		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC
					Venkataramakrishnan Vinnakota	BC Hydro and Power Authority	2	WECC
					Pat G. Harrington	BC Hydro and Power Authority	3	WECC
					Clement Ma	BC Hydro and Power Authority	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	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
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Quintin Lee	Eversource Energy	1	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Greg Campoli	NYISO	2	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Power	1,5	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Scott Miller	Scott Miller		SERC	MEAG Power	Roger Brand	MEAG Power	3	SERC
					David Weekley	MEAG Power	1	SERC
					Steven Grego	MEAG Power	5	SERC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Deborah McEndafffer	Midwest Energy, Inc	NA - Not Applicable	NA - Not Applicable
					Robert Gray	Board of Public Utilities (BPU) Kansas City, Kansas	3	SPP RE
					Louis Guidry	Cleco	1,3,5,6	SPP RE
					Megan Wagner	Westar Energy	6	SPP RE
PPL - Louisville Gas and Electric Co.	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
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE
ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					Sunflower Electric Power Corporation	SEPC	1	SPP RE
					Rayburn Country Electric Cooperative	RCEC	3	SPP RE
					Old Dominion Electric Cooperative	ODEC	3,4	SERC
					Brazos Electric Power Cooperative, Inc.	BRAZOS	1,5	Texas RE

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not "plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require the responsible entity's CIP Senior Manager to review and approve the controls adopted to meet the specific security objectives identified in the Reliability Standard at least every 15 months." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R3 addresses the Order No. 829 directive for requiring CIP Senior Manager review and approval of the plan. (P. 46). The SDT believes it is appropriate to allow entities to have flexibility in determining whether the CIP Senior Manager or delegate should review and approve the plan. CIP-003-6 provides for policy review by CIP Senior Manager only.	
Gregory Campoli - New York Independent System Operator - 2	
Answer	No

Document Name	
Comment	
Recommend removing those items covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy." The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely	

upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	No
Document Name	
Comment	
GRE supports the NRECA comments. In R1, NRECA recommends that the SDT reiterate "high and medium impact" each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to "products or services provided to the Responsible Entity," but 1.2.4 is not. We recommend adding this phrase to 1.2.4: "Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity." Further, we recommend further clarification to the term "vendor." We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term "vendor" is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term "system integrators" is not well understood and request further clarification.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

The main body text in Requirement R1 establishes applicability to high and medium impact BES Cyber Systems; the SDT believes repeating this applicability in the requirement parts is redundant. The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. Requirement R1 Part 1.2 pertains to procuring BES Cyber Systems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.

Timothy Reyher - Eversource Energy - 5	
Answer	No
Document Name	
Comment	

Comments:

Concerned that the R1 guidance provides details which are beyond the scope of R1

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.”

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Recommend removing those items (CIP-013 R1 subparts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance “double jeopardy.”

The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

{C}1.1 – Delete “planning for”. Or if the use of “planning for” in R1 creates a necessary distinction between 1.1 and 1.2, what is it?

- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn’t a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting?

-

- R1.2.2: "Coordination of responses to vendor-identified incidents….", it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided examples of processes related to Part 1.2.1 through 1.2.6 in the Implementation Guidance. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. The SDT agrees that some responsible entities may need to provide additional entity-specific clarifications in their cyber security risk management plans.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."

Part 1.1 and Part 1.2 address distinct directives from Order No. 829 pertaining to planning and procurement, respectively. (see Rationale and Order No. 829 P. 56 and P.59). Examples of processes or activities that could address the objectives for both are contained in the Implementation Guidance. Per Part 1.1, responsible entities must have process(es) that they use when planning for procurement of BES Cyber Systems to consider cyber security risks to the BES that could arise from transitions from one vendor to another vendor. The intent is for the responsible entity to consider cyber security risks that may result from the change in vendor, which may inform the entity's procurement process.

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE notes that the proposed standard is not responsive to the FERC directive. FERC Order No. 829 P. 59 specifically 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 Note in Requirement R2, however, states: "Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual *terms and conditions of a procurement contract*; and (2) vendor performance and adherence to a contract." Texas RE agrees that it is unreasonable to hold a registered entity accountable for a vendor's adherence to (or lack of adherence to) a contract. Texas RE agrees as the standard drafting team (SDT) claims obtaining specific controls in the negotiated contract may not be feasible at all times but Texas RE believes this is *best practice*. In fact, in most cases contracts for these types of systems typically include security provisions and set similar expectations as described in the standard. The proposed standards would prohibit the compliance monitor from verifying the registered entity implemented part 1.1 and sub-parts 1.2.1 through 1.2.7. Moreover, this verification is to ensure that the registered entities' plans are consistent with the contract's expectations and obligations of the parties.

Admittedly, there will be circumstances in which a contracts may not be consistent or silent as it pertains to the responsible entity's security management plans (e.g. existing contacts or contracts in which the responsible entity was unable to negotiate the appropriate terms into the contract.) In those circumstances, other evidence should be provided demonstrating that the responsible entity has processes to ensure the vendor is expected/obligated to act consistently with the responsible entity's cyber security risk management

plans as it relates to the vendor's products or services. Therefore, the contracts should remain in scope as to demonstrate the mapping of expectations from the plan to the contract as far as vendor interactions for those specific items included in the standard and to advance best practices leading to a more reliable BES.

Additionally, Texas RE has the following concerns:

- In the current CIP-013-1 version, the SDT elected to restrict the scope of the Supply Chain process to Medium and High Impact Bulk Electric System (BES) Cyber Systems, as well as exclude Physical Access Controls (PACS), Electronic Access Control and Monitoring Systems (EACMS), and Protected Cyber Assets (PCAs) from the scope of the Standard. In doing so, the SDT appeared to rely on a number of commenters that suggested that FERC Order No. 829, P. 59 excluded these types of devices. Specifically, these commenters pointed to the following language in the FERC Order: "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 Order No. 829, P. 59. Accordingly, it appears that the SDT has concluded that PACS, EACMS, and PCAs collectively do not fall within the scope of "industrial control system hardware" or "computing and networking services associated with bulk electric system operations."

  Texas RE is concerned PACS, EACMS, and PCAs *do* fall within the scope of "industrial control system hardware" and "computing and networking services associated with bulk electric system operations" as those terms are used in FERC Order No. 829. PACS, EACMS, and PCAs are foundational equipment within a network's architecture. Moreover, these devices are vendor supported and exposed to the precise vulnerabilities identified in FERC's supply chain directive. Given these facts, Texas RE does not believe there is either a basis in FERC Order No. 829 or, more importantly, a reliability-based rationale for excluding them from the scope of CIP-013-1.

- Page 7, Part 1.1: While FERC Order No. 829 specifically uses the term "hardware", Texas RE notes the word "hardware" is not used in the standard language. Texas RE recommends replacing the word equipment with the term hardware in order to be consistent with the FERC Order.

- Page 8, Section 1.2.6: Texas RE recommends the SDT define or provide examples of the term "*system-to-system remote access*" as this is a broad term which can be interpreted in many different ways.

Likes	0	

Dislikes 0	

Response. Thank you for your comment. The SDT believes proposed CIP-013-1 meets the reliability objectives contained in the project SAR and Order No. 829. The intent is for responsible entities to accomplish the objective by including the security topics contained in Requirement R1 Parts 1.2.1 – 1.2.6 in the entity's procurement processes, such as RFP or vendor negotiations. Evidence could include RFPs or other procurement correspondence that demonstrate the responsible entity's cyber security risk management concepts and controls. Consistent with the Order, the standard obligates responsible entities to address supply chain cyber security risk management without "directly impos[ing] obligations on suppliers, vendors or other entities that provide products or services to responsible entities" (P. 21). The note in Requirement R2 excludes contracts because the responsible entity may not be able to obtain all security provisions in Parts 1.2.1 – 1.2.6 with all vendors since the requirements cannot 'directly impose obligations on suppliers, vendors, or other entities".

The SDT believes that requiring entities to implement supply chain cyber security risk management plans for BES Cyber Systems provides the intended reliability benefit, which applies to "industrial control system hardware, software, and services associated with bulk electric system operations" as specified in Order No. 829 (P. 43). The SDT believes entities should have flexibility to determine supply chain cyber security risk management controls for other cyber assets, including EACMS, PACS, and PCAs. The SDT believes this is an appropriate risk-based approach that allows entities to focus resources where they provide the most reliability benefit. Although EACMS, PACS, and PCA do not fall within the scope of the proposed CIP-013-1 requirements, an entity may decide to use some of the supply chain cyber security risk management controls, processes, and procedures in planning and procuring for these assets as are used for applicable high and medium impact BES Cyber System.

The SDT does not believe changing 'equipment' to 'hardware' in the proposed standard will provide additional clarity.

Requirement R1 Part 1.6 addresses controls for all remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to "user-initiated access by a person", the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45).

Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	No

Document Name	
Comment	
AECI supports NRECA's comments provided below: In R1, NRECA recommends that the SDT reiterate "high and medium impact" each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to "products or services provided to the Responsible Entity," but 1.2.4 is not. We recommend adding this phrase to 1.2.4: "Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity." Further, we recommend further clarification to the term "vendor." We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term "vendor" is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term "system integrators" is not well understood and request further clarification.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The main body text in Requirement R1 establishes applicability to high and medium impact BES Cyber Systems; the SDT believes repeating this applicability in the requirement parts is redundant. The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1. The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. Requirement R1 Part 1.2 pertains to	

procuring BES Cyber Systems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.
Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment
GTC supports NRECA comments: In R1, NRECA recommends that the SDT reiterate "high and medium impact" each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to "products or services provided to the Responsible Entity," but 1.2.4 is not. We recommend adding this phrase to 1.2.4: "Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity." Further, we recommend further clarification to the term "vendor." We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term "vendor" is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term "system integrators" is not well understood and request further clarification.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The main body text in Requirement R1 establishes applicability to high and medium impact BES Cyber Systems; the SDT believes repeating this applicability in the requirement parts is redundant. The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1. The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. Requirement R1 Part 1.2 pertains to procuring BES Cyber Sytems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies Comments - NERC Cyber Supply Chain Risk Management 2016-03.docx
Comment	
The following comment covers several of the questions in one comment, submitted by the Foundation for Resilient Societies, Nashua, NH. (Comment at end of document)	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No

Document Name	
Comment	
ERCOT joins the comments of the IRC with the exception of the comment on Requirement R1, Part 1.1.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	

Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons:

- Is not performance based and therefore not auditable
- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013. However; the note in R2 should be maintained that states:

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

CHPD's reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

("new" meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term "elements" be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the "Rationale for R1" and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., "Each Responsible Entity shall and document the results of the assessment."). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has revised the CIP-013-1 Rationale and the Implementation Plan to address commenter concerns with some types of contracts including multi-party contracts and master agreements. The SDT believes proposed CIP-013-1 provides entities with the necessary flexibility to develop its plan such that it will cover the procurement actions used by the responsible entity. The SDT does not agree with removing procurement-related objectives from the proposed standard, or removing the examples of procurement processes from the Implementation Guidance, as several FERC directives in Order No. 829 are directly related to procurement. The SDT has revised the VSL for Requirement R1 to remove the word *elements.* Proposed CIP-013-1 contains *risk-based* requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The standard addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems. The SDT agrees that entities may be using other activities in other phases of the life cycle to also mitigate cyber security risks, and that some of these may be covered by other Reliability Standards.

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons: • Is not performance based and therefore not auditable	

- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to "contracts" and most references to "procurement" be struck from CIP-013. However; the note in R2 should be maintained that states:

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

CHPD's reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

("new" meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term "elements" be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the "Rationale for R1" and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., "Each Responsible Entity shall <insert performance activity> and document the results of the

assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has revised the CIP-013-1 Rationale and the Implementation Plan to address commenter concerns with some types of contracts including multi-party contracts and master agreements. The SDT believes proposed CIP-013-1 provides entities with the necessary flexibility to develop its plan such that it will cover the procurement actions used by the responsible entity. The SDT does not agree with removing procurement-related objectives from the proposed standard, or removing the examples of procurement processes from the Implementation Guidance, as several FERC directives in Order No. 829 are directly related to procurement. The SDT has revised the VSL for Requirement R1 to remove the word *elements.* Proposed CIP-013-1 contains *risk-based* requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The standard addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems. The SDT agrees that entities may be using other activities in other phases of the life cycle to also mitigate cyber security risks, and that some of these may be covered by other Reliability Standards.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	

Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons:

- Is not performance based and therefore not auditable
- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to "contracts" and most references to "procurement" be struck from CIP-013. However; the note in R2 should be maintained that states:

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

CHPD's reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

("new" meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term "elements" be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the "Rationale for R1" and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be

used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved. The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., "Each Responsible Entity shall <insert performance activity> and document the results of the assessment."). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has revised the CIP-013-1 Rationale and the Implementation Plan to address commenter concerns with some types of contracts including multi-party contracts and master agreements. The SDT believes proposed CIP-013-1 provides entities with the necessary flexibility to develop its plan such that it will cover the procurement actions used by the responsible entity. The SDT does not agree with removing procurement-related objectives from the proposed standard, or removing the examples of procurement processes from the Implementation Guidance, as several FERC directives in Order No. 829 are directly related to procurement. The SDT has revised the VSL for Requirement R1 to remove the word *elements.* Proposed CIP-013-1 contains *risk-based* requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The standard addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems. The SDT agrees that entities may be using other activities in other phases of the life cycle to also mitigate cyber security risks, and that some of these may be covered by other Reliability Standards.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No

Document Name	
Comment	

In the Response to Comments the SDT asserts “Identifying and assessing cyber security risks in BES Cyber System planning. The SDT revised CIP-013-1 Requirement R1 Part 1.1 to “specify risks that Responsible Entities shall consider in planning for procurement of BES Cyber Systems“. Previously, commenters indicated that “the scope of cyber security risks being addressed in R1 is unclear**”**. The SDT removed unnecessary and unclear wording from Requirement R1s main requirement and revised Requirement R1 Part 1.1 to clarify the supply chain cyber security risks that must be addressed by the Responsible Entity in planning for the procurement of BES Cyber Systems.”

This change does not clearly identify the risks as previously noted by commenters.

Dominion recommends the following language change for CIP-013-1, R1 Part 1.1:

“Include one or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess, if applicable, the cyber security risk(s) of (i) procuring and installing vendor equipment and software; (ii) network architecture security; and (iii) transitions between vendor”

Dominion also recommends the following proposed language change for CIP-013-1 R1 Part 1.2:

“One or more process(es) used during procurement of BES Cyber Systems that address the following, as applicable:”

R3 needs to contain the caveat found in R2 that “[Revision] of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders).”

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT believes the suggested addition of network architecture security to Part 1.1 is potentially unclear and could have a variety of interpretations by responsible entities. The SDT does not support the suggested change.

The SDT does not believe the suggested change from *in* to *during* for Part 1.2 provides additional clarity. Requirement R3 specifies that entities must review and obtain CIP Senior Manager approval of its plan. The SDT does not believe the note about implementation is appropriate for R3. The note in R2 applies to implementation of the entity's plan and is not limited to the initial plan only. If an entity revises its plan at a later date and implements the revised plan, it is not required to renegotiate or abrogate existing contracts as indicated by the note in R2.

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	

Comments: Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons:

- Is not performance based and therefore not auditable
- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to "contracts" and most references to "procurement" be struck from CIP-013. However; the note in R2 should be maintained that states:

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

CHPD's reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

("new" meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term "elements" be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the "Rationale for R1" and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., "Each Responsible Entity shall <insert performance activity> and document the results of the assessment."). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has revised the CIP-013-1 Rationale and the Implementation Plan to address commenter concerns with some types of contracts including multi-party contracts and master agreements. The SDT believes proposed CIP-013-1 provides entities with the necessary flexibility to develop its plan such that it will cover the procurement actions used by the responsible entity. The SDT does not agree with removing procurement-related objectives from the proposed standard, or removing the examples of procurement processes from the Implementation Guidance, as several FERC directives in Order No. 829 are directly related to procurement. The SDT has revised the VSL for Requirement R1 to remove the word *elements.* Proposed CIP-013-1 contains *risk-based* requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The standard addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems. The SDT agrees that entities may be using other activities in other phases of the life cycle to also mitigate cyber security risks, and that some of these may be covered by other Reliability Standards.	
Shawn Abrams - Santee Cooper - 1	
Answer	No
Document Name	
Comment	
The intent and purpose of CIP-013 is very dependent upon the Implementation Guidance document. We appreciate the hard work of the SDT to provide this document to industry and it has valuable information. A concern is that auditors can only audit to the requirements within the standard so some of the comments are based on needing more clarification within the standard itself. Language should be included in the standard (not just in the Rationale) that allows for inclusion of a clause in a procurement agreement stating that CIP-013 compliance must be met by the supplier unless it is either not offered or would significantly increase the cost of the agreement. (See CIP-013-1, Section B, Rationale for Requirement R1). This language in a procurement agreement, along with the supplier's stipulation that this compliance is either unavailable or will increase costs should constitute proof that CIP-013 compliance was considered by the Registered Entity but waived due to the supplier's inability to accommodate the requirement in a reasonable manner.	

The standard should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a supply chain cyber security risk management plan or plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Santee Cooper is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities.

This standard will create the need for entities to have an inventory tracking mechanism of products that are purchased under the supply chain risk management plan. For example, switches could be purchased for use in an IT department, not under the supply chain cyber security risk management plan, and this would preclude it from being used in a BES Cyber System. A CIP Exceptional circumstance or something similar should be added to the standard to allow an entity to use a piece of equipment not procured under the supply chain cyber security risk management plan rather than risk reliability of the BES.

Please add some wording to the requirement in the standard to address how far up the supply chain the plan applies to. If a laptop is purchased from a vendor is there an expectation that the cyber security risk management plan stop with that vendor or is there an expectation that the associated parts of the laptop fall under the plan? It's currently included in the rationale language but the rationale language cannot be audited.

What happens when a vendor is bought out by another vendor? Are you compliant until you have to negotiate a contract with the new vendor?

In R1 Parts 1.2.1 and 1.2.2, the term "vendor-identified incident" is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing "identified to "acknowledged" or "confirmed."

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The proposed CIP-013-1 requirements provide entities with flexibility to develop and implement an entity-specific cyber security supply chain risk management plan. The ERO Enterprise-endorsed Implementation Guidance provides examples of approaches to be compliant with the standard. As stated in NERC's approved Compliance Guidance Policy, "Registered entities can rely upon [the examples] and be reasonably assured that compliance requirements will be met."

Proposed CIP-013-1 does not preclude an entity from including a clause in a procurement agreement stating that CIP-013 compliance must be met by the supplier as suggested by the commenter. However, the SDT does not agree that this should be required by CIP-013 because it could negatively impact the procurement process for responsible entities. Furthermore, the SDT notes that the standard is not intended to impose obligations directly on the vendor. (P. 36)

The proposed requirements provide flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples. Some situations, such as when contracts are negotiated on behalf of the responsible entity, could be met by providing input to parties negotiating on behalf of the responsible entity.

Proposed CIP-013-1 address an entity's obligations to mitigate cyber security risks in planning and procuring high and medium impact BES Cyber Systems. An entity's inventory management, operating actions and management decisions to address emergency circumstances are not in scope of the standard. The SDT does not believe an exception such as CIP Exceptional Circumstances is needed to address equipment use. An entity could include provisions in its plan regarding procurement of products and services in emergency situations.

Procurement processes specified in Part 1.2 address various vendor-related cyber security topics. As noted in the Rationale section, the term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. The rationale section, including vendor description, becomes part of the guidelines section of the standard following board adoption. An entity can provide additional clarification of vendor relationships in its plan.

CIP-013 does not require an entity to renegotiate a contract when a vendor is bought by another vendor. However, if the entity negotiates a new contract after the effective date of CIP-013, that procurement process would fall under CIP-013.

Implementation Guidance provides examples of processes to address Parts 1.2.1 and 1.2.2 that provide additional clarity. A responsible entity can provide additional clarity if the responsible entity believes it is necessary in its cyber security supply chain risk management plan.	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Recommend modifying CIP-007 and CIP-010 to include the proposed risk management elements proposed in CIP-013, or take the corresponding elements out of CIP-007 and CIP-010 to make CIP-013 more than just having a plan. There are no quantifiable measures in CIP-013 that really justify it as a stand-alone standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Proposed CIP-013-1 contains risk-based requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The standard addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems. The SDT does not believe additional clarity or efficiencies will be gained by introducing new requirements for BES Cyber System planning and procurement into CIP-007 or CIP-010.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

Even though ReliabilityFirst believes the CIP-013-1 draft standard address directives from Federal Energy Regulatory Commission (FERC) Order No. 829 and is a positive step in addressing cyber supply chain management, ReliabilityFirst Abstains mainly due to Requirement R1 missing Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following specific comments for consideration.

1. Requirement R1

    i. Even though Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs) were not specifically called out specifically in FERC Order 829, ReliabilityFirst believes the SDT needs to examine the possible risk of not including EACMS, PACS and PCA as part of Requirement R1 and go beyond what was stated in FERC Order 829. EACMs and PACS are critical cyber assets that control access and monitoring into the entities' ESPs and PSPs and should follow the Supply Chain standard/requirements as do the High and Medium Impact Cyber Systems. As for the PCAs, if they are compromised due to a vulnerability in the vendors supplied hardware or software, they can possibly affect high and medium impact BES Cyber Systems. ReliabilityFirst offers the following modifications for consideration:

        a. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber System and, [if applicable, associated Electronic Access Control and Monitoring (EACM), Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA)]. The plan(s) shall include:

Likes 0	
Dislikes 0	

Response. The SDT believes that requiring entities to implement supply chain cyber security risk management plans for BES Cyber Systems provides the intended reliability benefit, which applies to "industrial control system hardware, software, and services associated with bulk electric system operations" as specified in Order No. 829 (P. 43). The SDT believes entities should have flexibility to determine supply chain cyber security risk management controls for other cyber assets, including EACMS, PACS, and PCAs. The SDT believes this is an appropriate risk-based approach that allows entities to focus resources where they provide the most reliability benefit. Although EACMS, PACS, and PCA do not fall within the scope of the proposed CIP-013-1 requirements, an entity may decide to use some of the supply chain

cyber security risk management controls, processes, and procedures in planning and procuring for these assets as are used for applicable high and medium impact BES Cyber System.	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

- BC Hydro appreciates the direction of the revisions ie to remove enforcement actions against responsible entities that have limited ability to influence vendors. However, BC Hydro still believes some aspects of R1 will be difficult to manage / enforce, especially given the breadth of vendors many responsible entities have associated with their BCAs. Not all vendors are going to be able to accommodate the asks of the requirement.
- "Notification by the vendor…" suggests the vendor is expected to reach out to the responsible entity, and communication / transparency is endorsed through potential inclusion of terms in RFP's / contracts. This relies on the vendor honesty / transparency and there is no way to verify their attestations. The requirement focuses on entities reviewing vendor processes which may have limited impact on reliability.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT believes responsible entities can meet the requirements of Part 1.2 and has provided some examples of ways to do so in the Implementation Guidance. The SDT agrees that responsible entities may not have the ability to obtain each of its desired cyber security controls in its contract with each of its vendors. The objective is to address the topics in Part 1.2 in the procurement process, with recognition that the actual terms and conditions of a contract are not in scope.

The SDT believes that engaging vendors to obtain notifications of relevant vulnerability and security issues can benefit reliability. For example, negotiations with vendors could lead to establishing designated points of contact for communicating issues. Responsible entities have flexibility to include entity-specific proposed terms and conditions in its plan.

Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
R1 states that each RE must have a plan with one or more processes that address ....as applicable. Applicability is in the eye-of-beholder, however the requirement does not specifically say as identified by the Responsibility Entity, which auditors may take as a deliberate act not to include, interpreting that it is not up to the Responsibilty Entity to determin which are applicable.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. In Part 1.2, 'as applicable' provides for situations where some of the topics do not apply to a given procurement action. For example, not all vendors will require remote access and therefore Part 1.2.3 and/or Part 1.2.6 do not apply.	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	No
Document Name	
Comment	
The clarification that we don't have and would like from NERC/WECC is the intent of the following statement in CIP-013 R1.2.5 ***"Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System".*** There is no Guidelines and technical basis at the end of the standard for this	

This has a very large implication as this says all software provided by a vendor has to perform an integrity and authenticity verification. This could implicate a dedicated channel from the vendor validating through software certificates which would imply entities forcing software vendors to provide this mechanism, which the likelihood of meeting this for MS, Symantec, (non-control system software) is slim. MD5 checksums can not validate the integrity of the software as this hashing mechanism was broken in 2005 (although a lot of software vendors still use it).	
Likes 0	
Dislikes 0	
Response. The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its procurement processes (such as in Requests for Proposal, contract negotiations, or other procurement processes). Part 1.2.5 does not obligate the responsible entity to obtain, or the vendor to provide, the means for performing software verification. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the terms and conditions ultimately negotiated by the parties and included in a contract. As a result, actual contract terms are not in scope for CIP-013.	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends the proposed standard differentiate between contractual and non-contractual purchases, such as commercial off-the-shelf (COTS) products or other purchases made without using a contract vehicle (e.g., credit card purchases or using repurposed equipment).	
Likes 0	

Dislikes 0	
Response. The proposed requirement provides flexibility for entities to distinguish cyber security risk management processes for various types of procurement activities in its plan. The SDT does not believe the standard should establish prescriptive requirements to differentiate. The SDT considers COTS procurements as a potential type of procurement to be addressed in the enity's plan.	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Requirement R1.

Oncor agrees with the concept; however, Oncor believes the language for R1.1 should be revised as follows, *"(i) Responsible Entity procures and installs vendor equipment and software"*; and *"(ii) Responsible Entity transitions from one vendor(s) product or service to another vendor(s) product or service".*

For Requirement 1.2.1., the current wording suggests that the vendor has sufficient knowledge of Oncor's environment to know that a particular vulnerability does in fact pose a security risk to Oncor. We offer a recommendation on the language, *"Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that could pose cyber security risk to the Responsible Entity;"*

Requirement 1.2.2. The current phrase "coordination of response" is not clear as to what is intended by "coordination". We offer a recommendation on the language, *"Coordination of response activities by the vendor and the Responsible Entity to address vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;"*

Requirement 1.2.3. The current wording suggests that the vendor has sufficient knowledge of Oncor to determine whether or not an individual should no longer be granted access. Oncor is the only party to an agreement that has the ability to determine who should or

should not have access. We offer a recommendation on the language, *"Circumstances where vendors should notify the Responsible Entity that access requirements of the vendor or third party personnel has changed, based on CIP-004, R5."*

Requirement 1.2.4. The current wording is not clear as to which vulnerabilities are applicable. We offer a recommendation on the language, *"Disclosure by vendors of known vulnerabilities in the procured product or service that follows a responsible disclosure process";* Guidance should also be added to reference US-CERT, NIST, or other industry sources.

Requirement 1.2.6. Oncor suggests the following wording change as the use of the phrase "Coordination of controls" is confusing. We offer a recommendation on the language, *"Controls for; (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)."*

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT does not believe the suggested wording for Part 1.1 provides additional clarity.

The SDT intends for the Parts 1.2.1 – 1.2.6 to list topics that must be addressed in the responsible entity's procurement processes, and has avoided more prescriptive wording. Responsible entities may provide entity-specific details and clarifications in their supply chain cyber security risk management plans.

Andrew Meyers - Bonneville Power Administration - 6	
Answer	No
Document Name	
Comment	

BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not

"plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require the responsible entity's CIP Senior Manager to review and approve the controls adopted to meet the specific security objectives identified in the Reliability Standard at least every 15 months." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R3 addresses the Order No. 829 directive for requiring CIP Senior Manager review and approval of the plan. (P. 46). The SDT believes it is appropriate to allow entity's flexibility in determining whether the CIP Senior Manager or delegate should review and approve the plan. CIP-003-6 provides for policy review by CIP Senior Manager only.	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
In R1, NRECA recommends that the SDT reiterate "high and medium impact" each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to "products or services provided to the Responsible Entity," but 1.2.4 is not. We recommend adding this phrase to 1.2.4: "Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity." Further, we recommend further clarification to the term "vendor." We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term "vendor" is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the	

term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term "system integrators" is not well understood and request further clarification.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The main body text in Requirement R1 establishes applicability to high and medium impact BES Cyber Systems; the SDT believes repeating this applicability in the requirement parts is redundant. The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1. The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. Requirement R1 Part 1.2 pertains to procuring BES Cyber Systems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Requirements R1 and R2 essentially shift the burden for ensuring that BES Cyber System hardware and software vendors, resellers, and integrators follow sound security management practices onto individual Responsible Entities, which N&ST considers both unfair and unreasonable, for small entities in particular. The just-endorsed (by NERC) CIP-013 Implementation Guidance document suggests an	

entity could address R1.1's requirement to "identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services" by means of a series of interactions with prospective vendors that comprise, for all intents and purposes, a risk assessment of the vendor, conducted by the entity. What recourse would a small entity have if a prospective supplier, perhaps the only one available, declined to cooperate with such an in-depth examination of its internal processes? R2, which requires the implementation of the entity's R1 plan(s), acknowledges a vendor may be disinclined to agree to contractual obligations to support one or more specific elements of an entity's R1 risk management plan. However, it contains no language that acknowledges this could make it difficult, if not impossible, for the entity to fully implement its R1 plan. N&ST believes this creates significant compliance risks for entities that may have few if any other options in some procurement situations. N&ST therefore recommends the addition of language similar to existing technical feasibility language in CIP-002 through CIP-011.

N&ST recommends that R2 be modified to state that a Responsible Entity has the option of describing its implementation of R1 Part 1.2.3 (revocation of vendor remote access privileges) in its CIP-004 Access Management and/or Access Revocation documentation.

N&ST recommends that R2 be modified to state that a Responsible Entity has the option of describing its implementation of R1 Part 1.2.6 (vendor remote access) in its CIP-005 ESP and Interactive Remote Access documentation.

N&ST recommends that R2 be modified to state that a Responsible Entity has the option of describing its implementation of R1 Part 1.2.5 (vendor software authenticity and integrity) in its CIP-010 Configuration Change Management documentation.

Initial CIP Senior Manager or delegate approval of risk management plan(s) should be added to R1. N&ST notes the initial implementation of R3 specified in the draft Implementation Plan is on or before the Effective Date. If that language is retained, there will be no need to add CIP Sr Manager or delegate approval to R1.

CIP-013 R2 and/or the Implementation Plan should contain "trigger" language for R2 that clarifies an entity must implement its R1 risk management plan(s) for new procurement contracts signed on or after the Effective Date of CIP-013. Entities with no new procurement contracts or no new in-progress procurements on the Effective Date should not be expected to be able to demonstrate compliance with R2 at that time.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT's approach with CIP-013-1 is consistent with Order No. 829, which directed NERC to develop requirements for NERC entities and to not impose obligations directly on vendors. The requirements provide responsible entities with flexibility to use tailored planning and procurement processes and do not obligate or hold the responsible entity accountable for vendor cooperation. The SDT believes the responsible entity can implement procurement processes as required by Part 1.2 without need for compliance exception because of the flexibility that is inherent in CIP-013. Examples of procurement processes are contained in the Implementation Guidance. Proposed CIP-013-1 Requirement R2 does not preclude the responsible entity from using the responsible entity's documentation related to other CIP standards. However, the documentation must demonstrate use of the responsible entity's supply chain cyber security risk management plan in procuring BES Cyber Systems. Proposed CIP-013-1 addresses initial approval of the responsible entity's plan through the Implementation Plan. The Implementation Plan specifies when an entity must begin using its plan, and has been revised for clarity (see Implementation Plan section). The SDT agrees that entities should not be expected to demonstrate compliance with Requirement R2 if the entity has not initiated procurement processes when the requirement is effective.

Don Schmit - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
NPPD supports the comments submitted by the MRO NSRF for CIP-013. In addition: NPPD is concerned that this Standard is not sufficiently represented to be auditable. First, the Standard is not performance based, which leads to auditor discretion, which leads to inconsistency among the Regional Entities across the NERC footprint. Second, the Implementation Guidance document has words that protect the entities from interpretation risk, however are not part of the Standard; which leaves the auditor to determine the intent of the drafting team. This is true in the rationale section for R1 which has wording which would minimize interpretation risk to entities, however are not reflected in the Standard. The Rationale states that the supplier must	

meet CIP-013 unless it is either not offered by the supplier or would significantly increase the cost of the agreement. This needs to be included in the Standard or as a footnote in the Standard. This would be very important to clarity in audit practices. In addition, the Standard should specifically state that as long as evidence demonstrates that all items expressly identified in R1 are contained in the "plan" and are implemented via R2 that entities shall not be out of compliance (there should be no findings for opinion on intent or security).

As with other recently produced CIP Standards, this Standard is being "rushed" to satisfy a FERC directive and without concise and clear wording, implementation considerations of all impacted parties, and the means for auditors to audit to a performance based Standard and understood audit practices. An extended comment/balloting period should be requested of NERC/FERC in order to produce an auditable Standard.

Other comments:

There are no parameters for Standard applicability. If a piece of equipment is purchased and the vendor and entity meet the Standard, do subsequent purchases of associated parts relative to the equipment or replacement parts of the equipment from other vendors need to also meet the Standard?

R1 Parts 1.2.1 and 1.2.2 "vendor-identified incident" is not clear. This needs to have clarity added in the Standard. In addition "identified" should be changed to "confirmed".

CIP-013 R1 parts 1.2.5 and 1.2.6 are covered in CIP-005 and CIP-010. CIP-013 parts 1.2.5 and 1.2.6 should be removed to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."

The responsible entity's supply chain cyber security risk management plan applies to high and medium impact BES Cyber Systems and must include procurement processes as specified in Part 1.2. The responsible entity is required to implement its plan, per Requirement R2. Any procurements of BES Cyber Systems including replacement of BES Cyber Systems, falls in scope of the entity's plan.

Implementation Guidance provides examples of processes to address Parts 1.2.1 and 1.2.2 that provide additional clarity. A responsible entity can provide additional clarity if the responsible entity believes it is necessary in its cyber security supply chain risk management plan.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

Guy Andrews - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC supports NRECA's Comments of:	

In R1, NRECA recommends that the SDT reiterate "high and medium impact" each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to "products or services provided to the Responsible Entity," but 1.2.4 is not. We recommend adding this phrase to 1.2.4: "Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity." Further, we recommend further clarification to the term "vendor." We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term "vendor" is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term "system integrators" is not well understood and request further clarification.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The main body text in Requirement R1 establishes applicability to high and medium impact BES Cyber Systems; the SDT believes repeating this applicability in the requirement parts is redundant. The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1. The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. Requirement R1 Part 1.2 pertains to procuring BES Cyber Systems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

Requirements 1.2 through 1.2.4. are extremely difficult to negotiate and implement with vendors, especially across such a diverse industry and diverse set of vendors. As written, the requirements make the vendor responsible for providing notifications to the Responsibility Entity. This puts the burden on the Responsible Entity to enforce these requirements through contractual obligations. The rationale states that "such contract enforcement is not subject to this Reliability Standard;" however, the performance of these requirements belongs solely to entities that are outside the jurisdiction of NERC and the Commission and can be held accountable only through contraction enforcement. As written, these specific reliability requirements put the Responsible Entities in a precarious position of acting as a surrogate regulator on a secondary industry.

If the intent is not to make the Responsible Entity accountable from a compliance stand point for the actions of vendors or other parties, the language should be written into the requirement wording. The clause in R2.2 states this exception, but does not then clarify what the Responsible Entity is obligated to do. The Responsible Entity is supposed to negotiate those terms, try to obtain that information, but if they can't then is it still not a violation? Will the auditors also look at it from this perspective?

Furthermore, the language of the R1.2 to R1.2.4 should be changed to meet the SDT's objectives while relying solely on the actions of the Responsible Entity and not those of any other party. However, if the intent is to include the items in R1.2 in the process for consideration of risk when selecting a vendor or product during the procurement process as the draft guidance seems to indicate, then those intentions should be explicit in the requirement language.

There is no issue with Requirement 3 requiring a periodic assessment of the supply chain cyber security risk management controls in order to update plans, etc. However, a recurring review by business unit stakeholders should be sufficient. The requirement to have the CIP Senior Manager or delegate approve the plan is simply a formality and is administrative in nature and provides no further security value.

Likes 0	

Dislikes 0	

Response. Thank you for your comments.

The SDT's approach in CIP-013-1 is in line with FERC Order No. 829, which stipulates that the standards should not impose obligations directly on vendors (P 36). The requirements provide responsible entities with flexibility to use tailored planning and procurement processes and do not obligate or hold the responsible entity accountable for vendor cooperation. The SDT believes the note in Requirement R2 establishes that terms and conditions, and vendor performance with contract provisions, are not in scope.
The SDT developed Implementation Guidance, which has been endorsed by the ERO Enterprise, to provide examples of compliant approaches to meet the requirements. As stated in NERC's approved Compliance Guidance Policy, "Registered entities can rely upon [the examples] and be reasonably assured that compliance requirements will be met."

The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of elements contained in the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. Examples are provided in the Implementation Guidance.

Requirement R3 addresses the Order No. 829 directive for requiring CIP Senior Manager review and approval of the plan. (P. 46).

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	

Comment

- Please provide clarification on what a "contract" is. For instance, is an annual software license a contract?
- Please provide feedback as to what Registered Entities should do if vendors refuse to the specifications within the CIP-013 requirements.

• Please provide further clarifications and expectations within Measure 2 to ensure entities are prepared for compliance oversight expectations.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The objective of Part 1.2 is for entities to include the listed topics in their supply chain cyber security risk management plans so that procurement and contract negotiation processes address the applicable risks. Contracts a a type of procurement vehicle used to obtain products and services. An annual software license can be a type of contract. The requirements provide responsible entities with flexibility to use tailored planning and procurement processes and do not obligate or hold the responsible entity accountable for vendor cooperation. Responsible entities have flexibility to address vendor responsiveness. The SDT believes the evidence listed in Measure M2 covers the various types of evidence that an entity would use in implementing its supply chain cyber security risk management plan to plan and procure BES Cyber Systems. Correspondence, policy documents, or working documents that can show how the entity implemented processes such as those listed in the Implementation Guidance to plan and procure applicable BES Cyber Systems could be used as evidence.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
SPP offers comments on the subrequirements of R1, as follows:	

R1.1 – SPP recommends that subpart (i) be modified to accommodate the procurement "and/or" installation of vendor equipment "and/or" software and, further, requests clarification as to the intended meaning of the "transitions from one vendor(s) to another vendor(s)" concept within the context of subpart (ii).

1.2.1 – SPP recommends that "products or services" be modified to reference "products and/or services."

1.2.2 – SPP requests clarification as to the "coordination" intended to be imposed, suggesting that the requirement may stand alone with any coordination component removed.

1.2.4 – SPP recommends that the 1.2.4 be modified to appropriately limit vendor disclosure of known vulnerabilities to the products and/or services provided to the Responsible Entity, consistent with 1.2.1. In addition, SPP notes that there is a lack of consistency between 1.2.1 and 1.2.4 with the use of the terms "vendor equipment" and "software" in 1.2.1, but uses the term "products" in subrequirement 1.2.4. SPP seeks clarification on whether the SDT intends "products" to be broader than equipment and software. SPP recommends that the SDT be consistent and use "vendor equipment" and "software" throughout, or provide additional clarification about the scope of the term "products."

1.2.6- SPP requests clarification as to the "coordination" intended to be imposed, suggesting that the requirement may stand alone with the coordination component removed. SPP believes the "coordination of controls" may be interpreted as requiring the Responsible Entity and vendor to jointly develop and/or coordinate controls, rather than simply requiring the Responsible Entity to address the requisite remote access controls in its supply chain cyber security risk management plan(s). As drafted, SPP is concerned that it is unclear what is required for "coordination," as well as how such coordination would be evidenced at audit.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT does not believe the suggested changes to Part 1.1 or 1.2.1 provide additional clarity.

The SDT has revised Part 1.2.4 for clarity. The SDT does not believe use of 'and/or' provides additional clarity.

The ERO Enterprise-endorsed Implementation Guidance lists examples of compliant approaches to Requirement R1 Parts 1.2, including 1.2.2 and 1.2.6. The SDT believes the standard and the examples in the Implementation Guidance provide the necessary clarity. Responsible Entities can provide additional detail in their Supply Chain Cyber Security Risk Management Plan.

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

NRG offers comments on the sub requirements of R1, as follows:

R1.1 – NRG recommends that subpart (i) be modified to accommodate the procurement "and/or" installation of vendor equipment "and/or" software and, further, requests clarification as to the intended meaning of the "transitions from one vendor(s) to another vendor(s)" concept within the context of subpart (ii).

1.2.1 – NRG recommends that "products or services" be modified to reference "products and/or services."

1.2.2 – NRG requests clarification as to the "coordination" intended to be imposed, suggesting that the requirement may stand alone with any coordination component removed.

1.2.4 – NRG recommends that the 1.2.4 be modified to appropriately limit vendor disclosure of known vulnerabilities to the products and/or services provided to the Responsible Entity, consistent with 1.2.1. In addition, NRG notes that there is a lack of consistency between 1.2.1 and 1.2.4 with the use of the terms "vendor equipment" and "software" in 1.2.1, but uses the term "products" in sub requirement 1.2.4. NRG seeks clarification on whether the SDT intends "products" to be broader than equipment and software. NRG recommends that the SDT be consistent and use "vendor equipment" and "software" throughout, or provide additional clarification about the scope of the term "products."

1.2.6- NRG requests clarification as to the "coordination" intended to be imposed, suggesting that the requirement may stand alone with the coordination component removed. NRG believes the "coordination of controls" may be interpreted as requiring the Responsible Entity and vendor to jointly develop and/or coordinate controls, rather than simply requiring the Responsible Entity to address the requisite remote access controls in its supply chain cyber security risk management plan(s). As drafted, NRG is concerned that it is unclear what is required for "coordination," as well as how such coordination would be evidenced at audit.

Additionally: NRG is concerned that the R1 guidance provides details which are beyond the scope of R1.

NRG requests that the NERC SDT consider re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. The Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term "vendor-identified incident" is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing "identified to "acknowledged" or "confirmed."

Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005.

Request more guidance for the term "vendor" and use cases. Guidance should prompt Entities to include their definition of "vendor" in their plan(s).

NRG recommends removing those items (CIP-013 R1 subparts 1.2.5 and 1.2.6) that are covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear that there is a remaining need for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

NRG requests SDT consideration that: The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, NRG requests NERC SDT consideration of the assertion that Registered Entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

CIP-013-1 R1.2 – "One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable: " The term "as applicable" implies it is optional. Who determines whether something is applicable or not? NRG suggests that NERC SDT remove it or provide additional clarity.

CIP-013-1 R1.2.3, NRG has concerns that it is not clear when vendors have to notify if remote or onsite access should no longer be granted to vendor representatives. 2 hrs, 24 hrs, or 3 months?

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

1.1 – Delete "planning for". Or if the use of "planning for" in R1 creates a necessary distinction between 1.1 and 1.2, what is it?

- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn't a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting?

-

- R1.2.2: "Coordination of responses to vendor-identified incidents….", it is not clear who should be doing the coordinating and why this is necessary. NRG requests SDT consideration of suggestion to delete.

Furthermore, NRG requests NERC SDT consideration of the following comments:

· On page 6 of CIP-013 draft:

NRG requests that the NERC standard drafting team consider providing additional clarification to the following paragraph:

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. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

NRG requests that industry have the ability to accept a level of risk through internal risk assessment processes if a supplier is unwilling to negotiate and accept the cyber security terms into negotiated contracts.

· On page 6 of CIP-013 draft:

NRG requests that the NERC standard drafting team consider providing additional clarification to the following paragraph:

A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

NRG requests that the term vendor be further clarified to specify if meaning developers, product resellers or system integrators of "third-party" software, system components, or information system services, etc (versus internal company developers).

· On page 8 of CIP-013 draft (under R2):

NRG requests that the NERC standard drafting team consider providing additional clarification to the following paragraph:

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

NRG requests further understanding of what, if any expectations are to be included in T&Cs and what are the expectations of how the vendor will be expected to perform as the term "expectations" is listed on page 6 of the standard?

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT does not believe the suggested changes to Part 1.1 or 1.2.1 provide additional clarity.

The SDT has revised Part 1.2.4 for clarity. The SDT does not believe use of 'and/or' provides additional clarity.

The ERO Enterprise-endorsed Implementation Guidance lists examples of compliant approaches to Requirement R1 Parts 1.2, including 1.2.2 and 1.2.6, that clarify the SDT's intent. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan. The ERO Enterprise endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. The SDT agrees that some responsible entities may need to provide additional entity-specific clarifications in their cyber security risk management plans.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. As previously stated, the ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. Accordingly, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations." (See Compliance Guidance Policy on NERC's compliance page)

Part 1.1 and Part 1.2 address distinct directives from Order No. 829 pertaining to planning and procurement, respectively. (see Rationale and Order No. 829 P. 56 and P.59). Examples of processes or activities that could address the objectives for both are contained in the Implementation Guidance.

Per Part 1.1, responsible entities must have process(es) that they use when planning for procurement of BES Cyber Systems to consider cyber security risks to the BES that could arise from transitions from one vendor to another vendor. The intent is for the responsible entity to consider cyber security risks that may result from the change in vendor, which may inform the entity's procurement process.

The SDT believes the cited paragraph "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…", along with the note in Requirement R2, addresses the commenter's concerns regarding the responsible entity's obligation when vendors may be unable or unwilling to negotiate. Implementation Guidance provides additional examples of compliant approaches that are not dependent on vendor cooperation. The SDT believes the vendor description provided in the rationale addresses the commenter concerns about internal company developers. The rationale section states, in part: *The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services.* A responsible entity can provide further clarification in its supply chain cyber security risk management plan if the responsible entity deems it necessary. As indicated in the note for Requirement R2, the following are not in scope for CIP-013: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	No
Document Name	
Comment	
CIP-005 has had R2.4 and R2.5 added as they pertain to interactive user access and remote system to system access tracking. These were previously in the CIP-013 standard as part of the Supply Chain requirement. Due to CIP-005 R2 already dealing with an Intermediate system for Interactive Remote access, it seems logical that this requirement be expanded to include these. The clarification that we don't have and would like from NERC/WECC is the intent of the following statement in CIP-013 R1.2.5 ***"Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System".*** There is no Guidelines and technical basis at the end of the standard for this	

This has a very large implication as this says all software provided by a vendor has to perform an integrity and authenticity verification. This could implicate a dedicated channel from the vendor validating through software certificates which would imply entities forcing software vendors to provide this mechanism, which the likelihood of meeting this for MS, Symantec, (non-control system software) is slim. MD5 checksums can not validate the integrity of the software as this hashing mechanism was broken in 2005 (although a lot of software vendors still use it). So we need clarification on this before a vote recommendation can be established for CIP-013 R1.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its procurement processes (such as in Requests for Proposal, contract negotiations, or other procurement processes). Part 1.2.5 does not obligate the responsible entity to obtain, or the vendor to provide, the means for performing software verification. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the terms and conditions ultimately negotiated by the parties and included in a contract. As a result, actual contract terms are not in scope for CIP-013.	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
PJM agrees, with the following suggested edits:	

Within 1.2.1 and 1.2.2, PJM feels that "incident" need further clarification as it is a bit broad (i.e. could be interpreted as anything from a phishing attempt to an actual breach). PJM suggests it be narrowed down to actual breaches. Additionally, "security risk to the Responsible Entity" should be "security risk to the BES." Lastly, we like how the notification and coordination pieces are split out. *Within 1.2.3, PJM suggests changing "no longer be granted" to "should be revoked" to strengthen the language.* *Within 1.2.5, PJM suggests adding in "firmware" and "where the method to do so is available" as to match the CIP-010 language.*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT does not believe the suggested changes to Part 1.2.1 – 1.2.3 provide additional clarity. The SDT understands *firmware* to be a type of software. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
The understanding of the intent and purpose of CIP-013 is very dependent on the Implementation Guidance document. There is no guarantee that this document will be approved by NERC even if CIP-013 is approved. Request clarification on whether the SDT intends "products" to be broader than equipment and software. Recommend that the SDT be consistent and use "vendor equipment" and "software" throughout, or provide additional clarification about the scope of the term "products."	

There are concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, we recommend that all references to "contracts" and most references to "procurement" be struck from CIP-013, except the note in R2 that states:

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

Our reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such we ask that R1.2 be revised as follows:

1.2. *One or more process(es) used in procuring for its newly procured BES Cyber Systems that address the following elements, as applicable:*

("new" meaning obtained after the implementation of CIP-013).

Request that the term "elements" be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the "Rationale for R1" and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits or subtext in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. There should be no expectation of what might or should be included within Requests for Proposals, no expectation of when contracts might or should be renegotiated, no expectations of what terms might or should be included or requested, and no expectations of what terms might or should be found in a prudent and proper contract. Ultimately, there should be no expectation that such protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

In the absence of such a change, we requests substantial additional clarification about how, without contract terms and contract negotiations being auditable, performance of R2 implementation will be audited and assessed.

Likes 0	
Dislikes 0	

Response Thank you for your comment.

The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities.

Vendor equipment and software are types of products. The SDT does not believe alternate wording for Requirement R1 provides additional clarity. A responsible entity may provide additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.

The SDT believes the requirements for procurement processes are necessary to address the Order No. 829 directives (P. 59). The proposed requirements provide flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples.

The SDT has revised the VSL for Requirement R2 to remove the word *element*.

The SDT believes the evidence listed in Measure M2 covers the various types of evidence that an entity would use in implementing its supply chain cyber security risk management plan to plan and procure BES Cyber Systems. Correspondence, policy documents, or working documents that can show how the entity implemented processes such as those listed in the Implementation Guidance to plan and procure applicable BES Cyber Systems could be used as evidence.

Implementation Guidance provides examples of processes to address Parts 1.2.1 and 1.2.2 that provide additional clarity. A responsible entity can provide additional clarity if the responsible entity believes it is necessary in its cyber security supply chain risk management plan.

Quintin Lee - Eversource Energy - 1

Answer	Yes
Document Name	
Comment	

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.

Recommend removing CIP-013 R1 subparts 1.2.5 and 1.2.6 from CIP-013 since these are covered in CIP-005 and CIP-010. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance “double jeopardy.”

The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

{C}1.1 – Delete “planning for”. Or if the use of “planning for” in R1 creates a necessary distinction between 1.1 and 1.2, what is it?

- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn't a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting? - R1.2.2: "Coordination of responses to vendor-identified incidents….", it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided examples of processes related to Part 1.2.1 through 1.2.6 in the Implementation Guidance. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. The SDT agrees that some responsible entities may need to provide additional entity-specific clarifications in their cyber security risk management plans.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."

Part 1.1 and Part 1.2 address distinct directives from Order No. 829 pertaining to planning and procurement, respectively. (see Rationale and Order No. 829 P. 56 and P.59). Examples of processes or activities that could address the objectives for both are contained in the Implementation Guidance. Per Part 1.1, responsible entities must have process(es) that they use when planning for procurement of BES Cyber Systems to consider cyber security risks to the BES that could arise from transitions from one vendor to another vendor. The intent is for the responsible entity to consider cyber security risks that may result from the change in vendor, which may inform the entity's procurement process.	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed requirements in CIP-013-1 subject to the below requests for clarification and recommended revisions/additions. · AZPS requests that the SDT consider and provide guidance regarding the applicability of the requirements of CIP-013-1 where the traditional procurement process is not applicable to a particular purchase. For example, software that is purchased from a retail source rather than a vendor is often purchased subject to existing retail terms and conditions and without the opportunity to negotiate additional terms and conditions around the procurement. · AZPS further recommends the following changes/additions: · Requirement 1.2.4 - "Disclosure by vendors of known vulnerabilities ***when they become known to the vendor.***" · Requirement 1.2.5 as written is duplicative with CIP-010; hence, AZPS recommends this Requirement be deleted or revised to address the process for software integrity and authenticity, rather than actual verification of those.	

· Requirement 1.2.6 – AZPS recommends removal of the word “coordination” and on the insertion of the term “identification” to address a process for identifying how a vendor handles controls. · Requirement R2 – evidence may not be available for items that are purchased form a retail source, as noted above. AZPS recommends an exception be identified for this purpose.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Proposed CIP-013-1 requires responsible entities to develop and implement a supply chain cyber security risk management plan for BES Cyber Systems that addresses the specified planning and procurement processes. The proposed requirements provide flexibility for entities to develop a plan that includes various types of processes used for procurement by the responsible entity, and to address the applicable topics listed in Parts 1.2.1 through 1.2.6. The SDT does not believe the proposed revision to Part 1.2.4 is needed to meet the objective. A responsible entity can include the clarification in its supply chain cyber security risk management plan. The proposed requirement in CIP-010-3 is operational in nature and not related to procurement. Therefore the CIP-013 requirement is not duplicative of the CIP-010-3. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT does not believe the propose wording for Part 1.2.6 provides additional clarity. A responsible entity can include the clarification in its supply chain cyber security risk management plan. The SDT believes a responsible entity should use its supply chain cyber security risk management plan for all procurements of high and medium impact BES Cyber Systems, and be able to provide evidence for assurance purposes.	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	

Answer	Yes
Document Name	
Comment	
Modify R1.2.5 as follows: "Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System when technically feasible; and". This will help address concerns with vendors such as Microsoft that pushes patches when they identify a need. Add language to address allowable exception in the event of CIP Exceptional Circumstances for R2 (e.g. patches issued with ransomware attack in-progress needed immediate action to be taken). Luminant would prefer that the CIP-013 standard be formatted similar to other CIP standards with the use of tables (e.g.CIP-004-6 Table R1).	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R1 Part 1.2.5 does not require entities to perform software verification, so the SDT does not believe it is necessary to include *when technically feasible*. In implementing its processes in Part 1.2, the responsible entity is not required to include topics in 1.2.1 – 1.2.6 that are not applicable to the item being procured. This would include applications that are not technically feasible. Likewise, the SDT does not believe CIP Exceptional Circumstances apply to implementation of an entity's supply chain cyber security risk management plan. Implementation of elements contained in the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and negotiation processes. Performance of patch management is addressed in other reliability standards and not in scope of CIP-013. The SDT does not believe a table format would provide additional clarity.	

Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG request clarification, regarding R1.2.4, of whom the vulnerability must be known by to require disclosure and that it only be for the vendor's own products and only those supplied to the Responsible Entity. As stands, it might be interpreted that vulnerabilities might not need to be disclosed until publicly known, for products the Responsible Entity doesn't have, or for vulnerabilities the vendor might know in products other than its own. Suggest changing to "Disclosure by the vendor of vulnerabilities known to the vendor concerning products and services supplied by the vendor to the Responsible entity. Requirement R1 Part 1.2.4 requires additional clarification for the type of "known vulnerabilities" Vendor definition is required to avoid ambiguity; does the term vendor apply for contract employees/augmented staff/outsourcers?	

Are the requirements R1-R3 enforceable in exceptional circumstances?	
Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1. A responsible entity can provide additional clarity if the responsible entity believes it is necessary in its cyber security supply chain risk management plan.

The rationale section, including vendor description, becomes part of the guidelines section of the standard following board adoption. An entity can provide additional clarification of vendor relationships in its plan. Requirement R1 Part 1.2 pertains to procuring BES Cyber Systems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.

The SDT considered whether to include provisions for CIP Exceptional Circumstances in Proposed CIP-013-1, but determined that the exceptions were not appropriate because CIP-013-1 addresses planning and procurement processes.

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
ACES supports the requirements to reduce the risk of remote access management. Using the CIP Applicability Section reduces the previous confusion of what BES Cyber Assets are in scope.	
Likes 0	

Dislikes 0	
Response. Thank you for your comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	

Concerned that the R1 guidance provides details which are beyond the scope of R1

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.”

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Recommend removing those items (CIP-013 R1 subparts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform

the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy." The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy. Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed? 1.1 – Delete "planning for". Or if the use of "planning for" in R1 creates a necessary distinction between 1.1 and 1.2, what is it? - What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn't a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting? - R1.2.2: "Coordination of responses to vendor-identified incidents….", it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response. Thank you for your comments. The examples provided in the Implementation Guidance demonstrate a way, but not the only way, of being compliant with CIP-013-1. The SDT believes the examples are in scope. Responsible entities are not obligated to use approaches in the Implementation Guidance. Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore	

the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
See below comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

No comment.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has provided examples of processes related to Part 1.2.1 through 1.2.6 in the Implementation Guidance. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
The Registered Entity suggests consider revising Section 1.2.3 to clarify under what circumstances vendors would be expected to notify the Registered Entity that vendor remotes access should be revoked. Regarding Section 1.2.4, suggest revising to clarify what type of vulnerabilities would be included in this disclosure.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT clarified Part 1.2.4 to apply to 'products or services provided to the Responsible Entity'. The SDT has provided examples of processes related to Part 1.2.3 in the Implementation Guidance. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.	

Bob Thomas - Illinois Municipal Electric Agency – 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
R1-R2 are clearly stated and provide for the development and implementation of the required CIP-013-1 cyber security plans. R3 sets a clear expectation for periodic reviews and approvals. From an auditor's perspective, requiring the first review and approval of the R1 plan on or before the effective date of CIP-013-1 (Implementation Plan, Initial Performance of Periodic Requirements section, p. 3) provides clear guidance to industry on implementation expectations.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Jeff Icke - Colorado Springs Utilities - 5	

Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Regarding the use of the term “vendor,” as described in the “Rationale for Requirement R1” section of CIP-013-1: the SDT may want to clarify that staff augmentation contractors are not considered to be “vendors” in the context of the standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	Yes
Document Name	

Comment
What is the difference between 1.2.1 and 1.2.4? Why is the scope of 1.2.2 limited to vendor-identified incidents? What if a third party identifies an incident? Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed? 1.1 – Delete “planning for”. Or if the use of “planning for” in R1 creates a necessary distinction between 1.1 and 1.2, what is it? - What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn’t a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting? - R1.2.2: “Coordination of responses to vendor-identified incidents….”, it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Examples for all of the parts in Part 1.2 are included in the Implementation Guidance. *Incidents* (Part 1.2.1) could be a security breach at a vendor; *vulnerabilities* (1.2.4) could be a product security flaw. Responsible entities can provide additional clarifications in their Supply Chain Cyber Security Risk Management Plans. Part 1.2.2 specifies that the responsible entity must have process used in procurement to address coordination of responses to vendor-identified incidents. The term *vendor-identified* is used because to indicate that the objective is to address those incidents that arise with the vendor from which the product or service is being procured. A responsible entity could choose to use alternate terms, such as third-party, or expand the scope in its Supply Chain Cyber Security Risk Management Plan.	

Part 1.1 and Part 1.2 address distinct directives from Order No. 829 pertaining to planning and procurement, respectively. (see Rationale and Order No. 829 P. 56 and P.59). Examples of processes or activities that could address the objectives for both are contained in the Implementation Guidance. Per Part 1.1, responsible entities must have process(es) that they use when planning for procurement of BES Cyber Systems to consider cyber security risks to the BES that could arise from transitions from one vendor to another vendor. The intent is for the responsible entity to consider cyber security risks that may result from the change in vendor, which may inform the entity's procurement process.

Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
With respect to the proposed Requirement 1 Part 1.2.1, compliance requires the vendor to be responsive to vendor-identified incidents. We can only be compliant if the vendor releases such information. We can't be held responsible for a vendor that does not provide incident related information. This verbiage has to be deemed acceptable when developing the plan(s). With respect to the proposed Requirement 1 Part 1.2.4, compliance requires the vendor to be responsive to disclosing vulnerabilities. We can only be compliant if the vendor releases such information. We can't be held responsible for a vendor that does not disclose vulnerabilities. This verbiage has to be deemed acceptable when developing the plan(s). With respect to the proposed Requirement 1 Part 1.2.5, compliance requires cooperation by the vendor to participate in such a program. We will give procurement preference to vendors willing to participate however we are still at relying on vendor cooperation. We can't be held responsible for a vendor that does not provide accurate verification of software integrity and authenticity. This verbiage has to be deemed acceptable when developing the plan(s).	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. Vendor performance or response does not determine responsible entity compliance with any parts in Part 1.2. Examples of compliant approaches are included in the Implementation Guidance.	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
We support the comments submitted by APPA, including the following recommendations: Re-word R1, Parts 1.2.1 and 1.2.4 to better describe what is expected. The endorsed Guidance does not adequately distinguish between the two parts. "Vendor" is not a NERC-defined term and contributes ambiguity. Those items (CIP-013 R1, Parts 1.2.5 and 1.2.6) covered in CIP-005 adn CIP-010 should be removed from CIP-013 to avoid duplication. The Compliance and/or Implementation Guidance should make clear that, when evidence demonstrates that all items expressly identified in CIP-013 R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. There is concern about language related to procurement contracts, specifically the use of master agreements, piggyback agreements, and evergreen agreements. All references to "contracts" and most references to 'procurement" should be struck from CIP-013, except the note in R2.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

The SDT revised Part 1.2.4 for consistency with other parts in Part 1.2. The SDT believes Part 1.2.1 and 1.2.4 meets the reliability objective of Order No. 829 and that the endorsed Implementation Guidance provides additional clarity by describing examples of compliant approaches to meet these parts. Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."

Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	
: Platte River Power Authority (PRPA) continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013. PRPA agrees with limiting the requirement to high and medium assets only.	

R1: PRPA generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities.

PRPA recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

R2: PRPA agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in Requirement 1.

R3: PRPA agrees that a 15-month review period is appropriate to review the supply chain cyber security risk management plan in Requirement 1.

Additionally, PRPA proposes that the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date. This is similar to when the regional entities performed transition period audits of CIP v5 programs.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Proposed Requirement R1 provides flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore

the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations." The SDT agrees that the ERO roll-out strategy for CIP-013 following regulatory approval should include activities to help responsible entities develop and assess their plans and promote consistency in audit approaches.	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
For Requirement R 1, Part 1.2.4, CenterPoint Energy Houston Electric, LLC ("CenterPoint Energy") recommends the following modification to help clarify the type of disclosed vulnerabilities: "Disclosure by vendors of known security vulnerabilities involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System."	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

The SDT revised Part 1.2.4 for consistency with other parts in Part 1.2. The SDT does not believe it is necessary to include 'or its supply chain' in the requirement since this could be covered by the requirement as written. A responsible entity could include such a clarification in its plan if the responsible entity so desires.	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Even though the second proposed version of this standard has been simplified, SDG&E believes compliance with CIP-013-1 is potentially difficult and costly to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
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 continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.

SMUD agrees with limiting the requirement to high and medium assets only.

R1: SMUD generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a Technical Feasibility Exception (TFE) or Asset Capability Exception, should be included in the standard for these kinds of procurement activities. An additional consideration is to allow agreements between the vendor and entity that will not cause a financial impact, such as a letter of understanding, commitment to a plan of action or other agreement.

SMUD recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Proposed Requirement R1 provides flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	

Austin Energy (AE) supports efforts to ensure the security of the Bulk Electric System and appreciates the time and effort the SDT put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.

AE agrees with limiting the requirement to high and medium assets.

R1: AE generally agrees with the proposed R1 but has concerns about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and "piggyback" agreements. NERC should include an exception, comparable to a CIP Exceptional Circumstance, for such procurement activities.

AE recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts which require entities to perform the underlying function and take those functions into account during the procurement process is needless duplication which does not increase security or reliability and could result in compliance “double jeopardy.”

R2: AE agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in R1.

R3: AE agrees a 15-month review period is appropriate to review the supply chain cyber security risk management plan in R1.

Additionally, AE proposes the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date, similar to when the regional entities performed transition period audits of CIP v5 programs.

Likes 0	
Dislikes 0	

Response Thank you for your comments. Proposed Requirement R1 provides flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples. Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations." The SDT agrees that the ERO roll-out strategy for CIP-013 following regulatory approval should include activities to help responsible entities develop and assess their plans and promote consistency in audit approaches.
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See attached comments	

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The proposed requirements provide flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples. Some situations, such as when contracts are negotiated on behalf of the responsible entity, could be met by providing input to parties negotiating on behalf of the responsible entity. Proposed CIP-013 does not preclude responsible entities from taking other actions suggested by the commenter to pursue cyber security protections.

The SDT does not believe removing the procurement and contracting process from the scope of the proposed standard would meet the project SAR and directives in Order No. 829, which direct NERC to develop standards to "require entities to develop and implement a plan that includes security controls for supply chain management" (P. 43) and to include certain procurement controls (P. 45). The intent is for responsible entities to accomplish the objective by including the security topics contained in Requirement R1 Parts 1.2.1 – 1.2.6 in the entity's procurement processes, such as RFP, vendor negotiations, or input into cooperative agreements. Evidence could include RFPs or other procurement correspondence that demonstrate the responsible entity's cyber security risk management concepts and controls. Consistent with the Order, the standard obligates responsible entities to address supply chain cyber security risk management without "directly impos[ing] obligations on suppliers, vendors or other entities that provide products or services to responsible entities" (P. 21).

The SDT developed Implementation Guidance, which has been endorsed by the ERO Enterprise, to provide examples of compliant approaches to meet the requirements. As stated in NERC's approved Compliance Guidance Policy, "Registered entities can rely upon [the examples] and be reasonably assured that compliance requirements will be met."

The SDT clarified Part 1.2.4 to apply to 'products or services provided to the Responsible Entity' for consistency with other parts in Part 1.2. Examples of approaches for Part 1.2.1 through 1.2.6 are provided in Implementation Guidance. Responsible entities can provide additional clarification in their supply chain cyber security risk management plans.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. The SDT agrees that some responsible entities may need to provide additional entity-specific clarifications in their cyber security risk management plans. Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
Concerned that the R1 guidance provides details which are beyond the scope of R1 Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005.	

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s). Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. Request to merge R1 Part 1.2.1 and 1.2.2 for the notification and the coordination related to vendor-identified incidents. Request to merge R1 Part 1.2.3 and Part 1.2.6 for the notification and the coordination of controls when remote or on site access are required and granted for (i) vendor-initiated interactive remote access, and (ii) system-to-system remote access with a vendor(s). The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity’s procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. The SDT agrees that some responsible entities may need to provide additional entity-specific clarifications in their cyber security risk management plans.

The SDT clarified Part 1.2.4 to apply to ‘products or services provided to the Responsible Entity’ for consistency with other parts in Part 1.2.

The SDT does not believe merging certain parts in Part 1.2 provides additional clarity.

The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."	
Theresa Allard - Minnkota Power Cooperative Inc. - 1	
Answer	Yes
Document Name	
Comment	
See MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.	

SRP agrees with limiting the requirement to high and medium assets only.

R1: SRP generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities.

SRP recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

R2: SRP agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in Requirement 1.

R3: SRP agrees that a 15-month review period is appropriate to review the supply chain cyber security risk management plan in Requirement 1.

Additionally, SRP proposes that the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date. This is similar to when the regional entities performed transition period audits of CIP v5 programs.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Proposed Requirement R1 provides flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations." The SDT agrees that the ERO roll-out strategy for CIP-013 following regulatory approval should include activities to help responsible entities develop and assess their plans and promote consistency in audit approaches.	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Even though the second proposed version of this standard has been simplified, SDG&E believes compliance with CIP-013-1 is potentially difficult and costly to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
While in overall agreement with Requirements 1 through 3, ACEC does have the following concern: The R1 and R2 requirements in the draft split the development of one or more documented supply chain cyber security risk management plan(s) (R1) and the implementation of those supply chain cyber security risk management plan(s) specified in Requirement R1 (R2). By splitting these the potential for violations have been increased from one (1) to two (2) – one for each requirement. It is recommended that R1 and R2 be combined to reduce the potential of multiple violations for what should be a single Requirement. To illustrate, a majority of the Standards have their development of plans, processes, or procedures and implementation of those plans, processes, or procedures in the same requirement: CIP-002-5.1 R1; CIP-003-6 R2, R4; CIP-004-6 R1, R2, R3, R4, R5; CIP-005-5 R1, R2; CIP-006-6 R1, R2, R3; CIP-007-6 R1, R2, R3, R4, R5; CIP-010-2 R1, R2, R3, R4; CIP-011-2 R1, R2	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. In developing the 2nd draft of proposed CIP-013-1, the SDT separated requirements for responsible entities to develop and implement their Supply Chain Cyber Security Risk Management Plans. The SDT believes this approach to CIP-013-1 clarifies the obligations and more straightforward for responsible entities.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	

Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
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, R1.2.4 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? 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, 1.2.2, 1.2.4, 1.2.5 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 CIP-010-3 R1.6). Entities typically use update or proxy servers to discover and identify applicable security patches. For example, some 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. Thank you for your comment. The SDT believes the proposed requirement as written accomplishes the reliability objectives contained in the project SAR and FERC Order No. 829. The intent is for responsible entities to accomplish the objective by including the security topics contained in Requirement R1 Parts 1.2.1 – 1.2.6 in the entity's procurement processes, such as RFP or vendor negotiations. Consistent with the Order, the standard obligates responsible entities to address supply chain cyber security risk management without "directly impos[ing] obligations on suppliers, vendors or other entities that provide products or services to responsible entities" (P. 21). The note in Requirement R2 excludes contracts because they may contain business-sensitive information, and because the responsible entity may not be able to obtain all security provisions in Parts 1.2.1 – 1.2.6 with all vendors since the requirements cannot 'directly impose obligations on suppliers, vendors, or other entities". Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The approved requirements for security patch management in CIP-007 and proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational and procurement related controls provide reliability benefit and are needed to address the directives in Order No. 829.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

There is a lack of consistency between R1 parts 1.2.1 and 1.2.4 with respect to the use of the terms. While part 1.2.1 uses the “vendor equipment” and “software,” part 1.2.4 uses the term “products.” The SDT should clarify if it intends “products” to be broader in scope than equipment and software. USI recommends that the SDT be consistent and use “vendor equipment” and “software” throughout, or provide additional clarification about the scope of the term “products.”

In R1 parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. USI suggests changing “identified to “acknowledged” or “confirmed.”

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

USI believes the SDT should provide guidance regarding the use of the term “vendor.” If “Vendor” is not defined by NERC, the Guidance should recommend that Entities include their definition of “vendor” in their plan(s).

Associated guidance in the “Rationale for R1” and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits or subtext in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. There should be no expectation of what might or should be included within Requests for Proposals, no expectation of when contracts might or should be renegotiated, no expectations of what terms might or should be included or requested, and no expectations of what terms might or should be found in a prudent and proper contract. Ultimately there should be no expectation that such protections be achieved solely through the procurement process. Consistent with performance-based standards the objective is achieving each protection, not in how it is achieved.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response. Thank you for your comment.

The SDT has addressed any inconsistent terms in parts 1.2.1 – 1.2.6 as appropriate.

The SDT does not believe changing 'identified' to 'confirmed' in part 1.2.1 provides additional clarity to the requirement. Responsible Entities have flexibility to tailor their supply chain cyber security risk management plans for clarity where deemed appropriate by the Responsible Entity. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard. The SDT does not agree that the guidance should recommend entities develop their own definition of vendor because entities can use the description that is included in the rationale. However, if an entity determines additional clarity is needed, they may provide such clarity in their supply chain cyber security risk management plan. Proposed CIP-013-1 contains *risk-based* requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The commenter's approach suggests removing the procurement and contracting process from the scope of the proposed standard. Such an approach would not meet the directives in Order No. 829, which direct NERC to develop standards to "require entities to develop and implement a plan that includes security controls for supply chain management" (P. 43) and to include certain procurement controls (P. 45). The intent is for responsible entities to accomplish the objective by including the security topics contained in Requirement R1 Parts 1.2.1 – 1.2.6 in the entity's procurement processes, such as RFP or vendor negotiations. Evidence could include RFPs or other procurement correspondence that demonstrate the responsible entity's cyber security risk management concepts and controls. Consistent with the Order, the standard obligates responsible entities to address supply chain cyber security risk management without "directly impos[ing] obligations on suppliers, vendors or other entities that provide products or services to responsible entities" (P. 21). .

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	

Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
ITC Holdings agrees with the proposed requirements, however, we believe the wording of CIP-013 leaves a lot of room for interpretation. We recommend being more prescriptive in the wording of CIP-013 as well as providing detailed guidance in the Technical Guidance document. Additionally, ITC Holdings agrees with the below comment submitted by SPP regarding the use of "coordination": 1.2.6- SPP requests clarification as to the "coordination" intended to be imposed, suggesting that the requirement may stand alone with the coordination component removed. SPP believes the "coordination of controls" may be interpreted as requiring the Responsible Entity and vendor to jointly develop and/or coordinate controls, rather than simply requiring the Responsible Entity to address the requisite remote access controls in its supply chain cyber security risk management plan(s). As drafted, SPP is concerned that it is unclear what is required for "coordination," as well as how such coordination would be evidenced at audit.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT's intent with proposed CIP-013-1 is to address the reliability objectives in the project SAR and Order No. 829 in a non-prescriptive manner. To provide a clear example of compliance with the standard, the SDT developed Implementation Guidance what has been endorsed by the ERO Enterprise in accordance with NERC's Compliance Guidance policy.	

The ERO Enterprise-endorsed Implementation Guidance lists examples of compliant approaches to Requirement R1 Part 1.2, including 1.2.2 and 1.2.6. The SDT believes the standard and the examples in the Implementation Guidance provide the necessary clarity. Responsible Entities can provide additional detail in their Supply Chain Cyber Security Risk Management Plan.
Wesley Maurer - Lower Colorado River Authority - 5

Answer	Yes
Document Name	
Comment	
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	
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	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 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	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 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	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	

David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	

Requirement R1. The IRC has no issues with the concept. We offer a recommendation on the language, "(i) Responsible Entity procures and installs vendor equipment and software; and (ii) Responsible Entity transitions from one vendor(s) product or service to another vendor(s) product or service".

Note: **ERCOT does not support the above comment.**

Requirement 1.2.1. The current wording suggests that the vendor has sufficient knowledge of the Responsible Entities' environment to know that a particular vulnerability does in fact pose a security risk to the Responsible Entity. We offer a recommendation on the language, *"Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that could pose cyber security risk to the Responsible Entity;"*

Requirement 1.2.2. The current phrase "coordination of response" is not clear as to what is intended by "coordination". We offer a recommendation on the language, *"Coordination of response activities by the vendor and the Responsible Entity to address vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;"*

Requirement 1.2.4. The current wording is not clear as to which vulnerabilities are applicable. We offer a recommendation on the language, *"Disclosure by vendors of known vulnerabilities in the procured product or service following a responsible disclosure process"."*

Requirement 1.2.6. The use of the phrase "Coordination of controls" is confusing. We offer a recommendation on the language, *"Controls for; (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)."*

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT believes Parts 1.2.1 – 1.2.6 describe the cyber security risk topics that must be included in each responsible entity's Supply Chain Cyber Security Risk Management Plan for use in procuring BES Cyber Systems. Responsible entities can tailor specific wording in their plan to meet their procurement needs or to conform to the responsible entity's cyber security policies, plans, and practices.	
IESO	
Answer	No
Document Name	
Comment	
The IESO agrees in principle with the proposed requirements and respectfully submit suggestions for purposes of clarity. Requirement 1.2.1 We suggest the following wording change as the current wording suggests that the vendor has sufficient knowledge of the Responsible Entities' environment to know that a particular vulnerability does in fact pose a security risk to the Responsible Entity. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that *could* pose cyber security risk to the Responsible Entity; Requirement 1.2.2 We suggest the following wording change as the current phrase "coordination of response" is not clear as to what is intended by "coordination". Coordination of response *activities by the vendor and the Responsible Entity* to address vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	

Requirement 1.2.3 We suggest the following wording change as the current wording suggests that the Vendor has sufficient knowledge of the Responsible Entity to determine whether or not an individual should no longer be granted access. The Responsible Entity is the only party to an agreement that has the ability to determine who should or should not have access. *Circumstances where vendors should notify the Responsible Entity that access requirements of the vendor or third party personnel has changed.* Requirement 1.2.4 We suggest the following wording change as the current wording is not clear as to which vulnerabilities are applicable. Disclosure by vendors of known vulnerabilities *in the procured product or service;* Requirement 1.2.6 We suggest the following wording change as the use of the phrase “Coordination of controls” is confusing. Controls for; (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes Parts 1.2.1 – 1.2.6 describe the cyber security risk topics that must be included in each responsible entity’s Supply Chain Cyber Security Risk Management Plan for use in procuring BES Cyber Systems. Responsible entities can tailor specific wording in their plan to meet their procurement needs or to conform to the responsible entity’s cyber security policies, plans, and practices.	
Richard Vine - California ISO - 2	
Answer	

Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank for your comment.	
W. Dwayne Preston - Austin Energy - 3	
Answer	
Document Name	
Comment	
I would support the comments of Andrew Gallo Austin Energy for all questions.	
Likes 0	
Dislikes 0	
Response. Thank for your comment.	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	

MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank for your comment.	

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the 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. The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT joins the comments of the IRC and offers the following additional comments:

Regarding Part 2.4, ERCOT is concerned that the meaning of "determining" in the phrase "have one or more methods for determining active vendor remote access sessions" is unclear. If the SDT's intent is to require *identification* of instances of active vendor remote access, ERCOT suggests rewording to "have one or more methods of *identifying instances of* active vendor remote access (including Interactive Remote Access and system-to-system remote access)."

ERCOT also requests clarification on the meaning of "system-to-system remote access." Interpreted broadly, this requirement could mean all ingress/egress network connections to the security zone. Identifying each instance of connection could become extremely burdensome, without providing any meaningful reliability benefit.

ERCOT recommends that the meaning of system-to-system remote access be qualified as vendor remote access which can do harm to the BES Cyber System (BCS) and recommends the following language:

"Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access). This is limited to sessions which have the ability to harm the BCS."

If the SDT declines to adopt this language, the SDT should consider defining "system-to-system remote access" or further clarifying the meaning of this term in the "Guideline and Technical Basis" section or in the Implementation Guidance.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The SDT does not believe replacing *determining* with *identifying instances* provides additional clarity. Requirement R2 Parts 2.4 and 2.5 address controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to "user-initiated access by a person", the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45). Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i)is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor. The SDT does not support the suggested change to include the sentence *This is limited to sessions which have the ability to harm the BCS* because the sentence could be inconsistently interpreted. The SDT believes the measures provide a list of some methods that can achieve the reliability objective without excessive burden on the Responsible Entity. For example, methods for accessing logged or monitoring information to determine active vendor remote access sessions may leverage existing entity processes.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	

See comments in attached file (comment at end of document)	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
It remains unclear to us as to what the phrase “system-to-system” is meant to include. Please define or provide examples of what would be considered vendor “system-to-system” remote access.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R2 Parts 2.4 and 2.5 address controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to “user-initiated access by a person”, the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45). Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i)is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor	
Timothy Reyher - Eversource Energy – 5	

Answer	No
Document Name	
Comment	

Comments:

The definition of vendor is crucial to an entity defining and carrying out its compliance objectives for the requirements in question.

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-013.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5

Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.

The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard.

The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy requests additional clarity pertaining to the use of the term “active” in Requirement 2 Parts 2.4 and 2.5. As written, it could be interpreted that an entity would be required to monitor the remote access sessions of a vendor in real-time. Was this the drafting team’s intent with this language? If the drafting team’s intent was that an entity only be able to identify which vendor’s have remote access, we suggest revising the standard to more closely reflect said intent. If it is the drafting team’s intent that an entity must monitor in real-time the remote access of a vendor, additional guidance as to acceptable methods to achieve compliance with this intent is necessary.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT’s intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. Meeting this objective does not require monitoring of remote access sessions in real time. The examples of evidence included in the Measures for Part 2.4 indicate that this method does not require monitoring of individual remote access sessions with a vendor in real time. Examples listed in the measure include:

- *Methods for accessing logged or monitoring information to determine active vendor remote access sessions;*
- *Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or*
- *Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.*

Don Schmit - Nebraska Public Power District – 5	
Answer	No
Document Name	
Comment	
NPPD supports the comments for the MRO NSRF for this question.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Nicholas Lauriat - Network and Security Technologies – 1	
Answer	No
Document Name	
Comment	
Suggest rewording 2.4 to read, “Have one or more methods for determining when vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) are active.” Alternative wording would be, “Have one or more methods for identifying active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT does not believe the suggested changes provide additional clarity.	

Wendy Center - U.S. Bureau of Reclamation – 5	
Answer	No
Document Name	
Comment	
Reclamation recommends that CIP-005-6 Requirement R2 Part 2.4 Requirements be changed to state, “Have one or more methods for determining and logging active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).” Reclamation recommends that the first bullet in CIP-005-6 Requirement R2 Part 2.4 Measures be changed to state, “Methods for accessing logged and actively monitored information to determine active vendor remote access sessions;” Reclamation also recommends that CIP-005-6 R2.3 be changed to "Where technically feasible, require multi-factor authentication for all Interactive Remote Access sessions" to align with CIP-007 R5, dealing with authentication requirements to help with consistency within the standards.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed Part 2.4 and 2.5 address the objectives contained in the project SAR and Order No. 829. These objectives are aimed at establishing controls on vendor remote access to BES Cyber Systems, covering both user-initiated and machine-to-machine vendor remote access, to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES (P. 51). The SDT does not believe the requirement needs to include logging to meet the objective. The SDT also does not believe the suggested change in M2 to *actively* monitored information improves the clarity of the requirement or effectiveness in addressing the objective. Modifying Requirement R2 Part 2.3 to address technical feasibility is not in scope for Project 2016-03 per the project SAR.	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	No
Document Name	
Comment	

CIP-005-6 R2 Part 2.4 as drafted does not identify the "direction" of how system-to-system remote access is initiated. Interactive Remote Access specifies that it originates "from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeters". Without defining the system of origin or other defining controls, similar to the definition of Interactive Remote Access, any connection from a CIP Cyber Asset to a vendor system, even if one-way and simply for data acquisition/submission, could be interpreted as subject to this requirement. Additional clarification is requested.

Additionally, the Supplemental Material for the requirement points to a separate document without an official link. It appears this document has not been updated in six (6) years, and mostly targets securing Interactive Remote Access. It is requested that updated relevant material be placed in the Standard's Supplemental Material section, similar to other CIP standards, and that the Supplemental Material section also attempt to provide guidance on the securing of system-to-system remote access.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

Requirement R2 Parts 2.4 and 2.5 address controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to "user-initiated access by a person", the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45). Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors, regardless of origin. System to system remote access is any remote access that: (i)is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor

The SDT has provided relevant information in the rationale section, which will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT believes Requirements R2 Part 2.4 and 2.5 and the accompanying measures, along with the rationale, provide the information necessary for entities to meet the reliability objective.	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
I fully support the concept of monitoring and being able to terminate all remote acccess sessions, however as written the additional requirements have no timing aspects associated with them, have no component for notification or alerting on active sessions, are atrifically limited to vendor access only, (lower case vendor) so may not include contractors, service providers, etc. Cannot support the requirement as written.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes the proposed requirements as written provide reliability benefit and address the Order No. 829 directives. Furthermore, CIP-005-6 Requirement R1 Part 1.5 provides a mechanism for Responsible Entities to determine when a response to suspicious activity in a vendor remote access session may be warranted. Part 1.5 requires Responsible Entities to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. Detections associated with this requirement could provide the triggering mechanism for Part 2.4.	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No

Document Name	
Comment	
With the deletion of the language in R2, it now appears that every Responsible Entity needs to have a documented process for Interactive Remote Access, even if the Responsible Entity does not allow it. Why did the team delete this exemption language from R2 as it seemed to lessen the burden for those entities that do not allow Interactive Remote Access?	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT developed Proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address Order No. 829 directives for vendor remote access controls with input from the Project 2016-02 CIP Revisions SDT. The scope of the revised requirement R2 is expanded to address all remote access management, not just Interactive Remote Access. It is not the intent of the SDT to require entities to have documented processes for remote access if the entity does not allow remote access. The SDT has added clarification to the Rationale section.	
Thomas Foltz - AEP – 5	
Answer	No
Document Name	
Comment	
R2 part 2.4 should read: Have one or more methods for determining when vendor Interactive Remote Access and/or vendor system-to-system remote access sessions are active. Part 2.5 should read: Have one or more methods to disable active vendor Interactive Remote Access and/or vendor system-to-system remote access sessions).	
Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT does not believe the suggested change provides additional clarity.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

The inclusion of (including Interactive Remote Access and system-to-system remote access) is problematic as the NERC defined term of Interactive Remote Access (IRA) explicitly excludes system-to-system process communication. Additionally, IRA already includes the concept of vendors (see 3) below).

"User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications."

The SDT should consider removing this system-to-system exclusion from the IRA defined term and stating Part 2.4 as –

Have one or more methods for determining active vendor Interactive Remote Access sessions.

And Part 2.5 as –

Have one or more method(s) to disable active vendor Interactive Remote Access sessions.

(note: the addition of 'sessions' in this Part to be consistent with Part 2.4.)

Lastly, from an SCRM perspective, the SDT should consider at least including some indication of when vendor remote access could or should be disrupted, but that may be better addressed in the CIP-013-1 R1.2.2 and/or R1.2.6 processes of the SCRM plan(s).	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees that revising the definition of IRA could have met the objective. However because the scope and application of the IRA term is beyond the scope of Project 2016-03, the SDT decided to address the vendor remote access objectives by using the approved defined term and adding system-to-system vendor remote access in the requirements. Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. The SDT believes CIP-005-6 Requirement R1 Part 1.5 provides a mechanism for Responsible Entities to determine when a response to suspicious activity in a vendor remote access session is warranted. Part 1.5 requires Responsible Entities to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	
Richard Vine - California ISO – 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Franklin Lu - Snohomish County PUD No. 1 – 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	

Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes

Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Please clarify definition of system-system communications.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R2 Parts 2.4 and 2.5 address controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to "user-initiated access by a person", the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45). Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i)is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor.	

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

There needs to be a clear explanation of “machine-to-machine” and “system-to-system” remote access in the Guidelines & Technical Basis to provide the necessary understanding and scoping of these concepts for industry.

For example – “Machine-to-machine” or “system-to-system” remote access would include a logical connection between a High or Medium Impact BES Cyber System or it’s associated PCAs into or out of the associated ESP with a vendor-maintained Cyber Asset, and that connection does not have an interactive user access capability.

Additionally, under the Measures of R2.4, the statement of examples needs to have “such as” following “(including Interactive Remote Access and system-to-system remote access), such as:” to make it clearer that the below bulleted items are options an entity may choose from, and to be consistent with the formatting of R2.5.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT is including the following clarification of vendor remote access in the rationale section to support Requirement R2 Parts 2.4 and 2.5: *Active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i)is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor.* The rationale section remains with the approved standard.

The SDT has made the suggested change to the Measure for Part 2.4.

David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
The IRC agree with the new CIP-005-6 Requirement R2 Parts 2.4 and 2.5 however we note there is no corresponding "Guidance and Technical Basis" or "Rationale". We also suggest that guidance be drafted to help entities understand what is intended by the term "Vendor" in relation to parts 2.4 and 2.5. Regarding Part 2.4, the IRC is concerned that the meaning of "determining" in the phrase "have one or more methods for determining active vendor remote access sessions" is unclear. If the SDT's intent is to require *identification* of instances of active vendor remote access, the IRC suggests rewording to "have one or more methods of *identifying instances of* active vendor remote access (including Interactive Remote Access and system-to-system remote access)."	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has provided relevant information in the rationale section, which will become part of the supplemental material following NERC Board adoption of the proposed standard. Rationale includes a description of vendor. Upon adoption of the standard by the NERC Board of Trustees, this information will be transferred to the guidelines section of the standard. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The SDT does not believe replacing *determining* with *identifying instances* provides additional clarity.	
IESO	
Answer	Yes

Document Name	
Comment	
The IESO agree with the new CIP-005-6 Requirement R2 Parts 2.4 and 2.5 however we note there is no corresponding “Guidance and Technical Basis” or “Rationale”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has provided relevant information in the rationale section, which will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT believes Requirements R2 Part 2.4 and 2.5 and the accompanying measures, along with the rationale, provide the information necessary for entities to meet the reliability objective	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
GTC supports NRECA comments: NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. It is not the intent of the SDT to require entities to have documented processes for remote access if the entity does not allow remote access. The SDT has added clarification to the Rationale section. The rationale remains in the standard following approval.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
The definition of vendor is crucial to an entity defining and carrying out its compliance objectives for the requirements in question. Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-013. Request more guidance for the term "vendor" and use cases. Guidance should prompt Entities to include their definition of "vendor" in their plan(s). Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5 Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response. Thank you for your comments. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.	

The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.	
Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
AECI supports NRECA's comments provided below: NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. It is not the intent of the SDT to require entities to have documented processes for remote access if the entity does not allow remote access. The SDT has added clarification to the Rationale section. The rationale remains in the standard following approval.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Texas RE agrees with the proposed requirements and has the following comments.

- Question 2 above uses the term "*machine-to-machine vendor remote access*". CIP-013-1 and CIP-005-6 use the term ""system-to-system remote access". Since these are two different terms, Texas RE recommends these terms be defined or examples provided to increase clarity and to avoid multiple interpretations.
- Section 4.2.3.5 – The language, "*Each Responsible Entity shall implement develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems*." is redundant with the requirement language. Also, neither CIP-013-1 nor CIP-010-3 contain this language in the Exemptions section.
- Page 1 Section 4.1.2.2 and Page 2 Section 4.2.1.2: Texas RE noted the term "*Special Protection System"* was removed. Texas RE recommends removing this term in all CIP standards.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT is using the term *system-to-system* for consistency with other NERC Reliability Standards and definitions. Additional description has been added to the rationale section.

Section 4.2.3.5 has been maintained from approved CIP-005-5.

NERC is incorporating the approved definition of Special Protection System into the body of standards through the course of ongoing and future projects.

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes

Document Name	
Comment	
The requirement in CIP-005-5 6 Table R2.4 states that an entity must have one or more processes to determine active vendor session. We would recommend adding 'Active and Passive' to the requirement since the Measures point to passive initiation in having the vendor call or receive permission before their remote access is granted. Additional guidance on what is 'Active' and whether the monitoring session requires tracking the entire session or initiation of the session would provide more clarity to industry.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT's intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. The SDT has added clarifying details to the rationale section. This material remains with the standard following approval.	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG suggest the term "vendor" be defined to exclude outsourcers that manage most aspects of a BES Cyber System. Normally they are contractually obligated to act in the Responsible Entities interests and fulfill or accommodate all compliance requirements. As such, this is a much closer relationship than is typically associated with the term "vendor". Because in many such cases they would be principle maintainer or operator of said systems would often not technically feasible to disable the outsourcer's access, remote or otherwise. Requirement 2.4 mentions ability to determine "sessions", not just "access". Requirement 2.5 is ambiguous on whether it requires the ability to disable "active sessions" as opposed to merely disabling "active accounts". Suggest replacing "access" in R2.5 with either "sessions" or "accounts" depending on what was intended or otherwise elaborating.	

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Requirement R2 Parts 2.4 and 2.5 are intended to mitigate risks of a compromise at a vendor from traversing over a network connection and impacting BES Cyber Systems (Order No. 829 P. 52). Depending on the responsible entity's arrangements with the vendor, outsourcer management of a Responsible Entity's BES Cyber System may not be within the scope of Parts 2.4 and 2.5. These requirement parts apply to Interactive Remote Access with a vendor and system-to-system remote access with a vendor. The SDT has clarified in the rationale section that the phrase *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i) is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (ii) is not IRA, and (iii) occurs between the Responsible Entity and a vendor. The SDT believes that contractors performing functions such as staff augmentation in a manner similar to an entity's own employee would not fall within the scope of Part 2.4.

As stated in the rationale, the objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52). The SDT believes the requirement and rationale are clear.

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski

Answer	Yes
Document Name	

Comment

GRE requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT has added clarification to the Rationale section. The rationale remains in the standard following approval.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the inclusion of Parts 2.4 and 2.5 within CIP-005-6 R2; however, requests the statement “active vendor remote access sessions” be changed to “active vendor remote connection.” A vendor may sustain an active remote connection for longer than an individual active remote access session. Thus, a revision to the language would clarify the intent of this requirement, which is to monitor any time a vendor is connecting to and accessing sensitive cyber assets remotely. Thus, AZPS encourages the SDT to consider this revision as it will better ensure that active remote connections by vendors are monitored and addressed.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes Part 2.4 and 2.5 are clear as written.	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Recommend creating a CIP-005-6 and CIP-010-3 ‘Guidance document’ similar to the one for CIP-013-1. Request that the narrative for the term 'Vendor' that is in the CIP-005-6 R2 Rationale box be added to the already Endorsed Guidance document for CIP-013-1 and to the Guidance documents for CIP-005-6 if it is created. Request that a narrative for the term 'System-to-System’ be added to the already Endorsed Guidance document for CIP-013-1 and to the Guidance documents for CIP-005-6 if it is created. Recommend removing CIP-013 R1 subparts 1.2.6 from CIP-013 since it is covered in the proposed CIP-005-6. Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5 Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the added parts (Part 2.4 and 2.5) and associated measures, and the rationale section, identify the responsible entity’s obligations and provide flexibility for the responsible entity to meet the vendor remote access reliability objectives identified in the project SAR. The rationale section remains in the standard following approval. The SDT believes they	

have fulfilled the tasks in the SAR and are not intending to develop Implementation Guidance for CIP-005-6 Requirement R2 Parts 2.4 and 2.5. Per NERC's Compliance Guidance Policy, registered entities may develop examples or approaches for complying with Reliability Standard requirements and vet them through an approved organization for ERO Enterprise endorsement consideration. The SDT has provided a description of *vendor* in the rationale section and has clarified the meaning of *system-to-system*. Rationale that is drafted during standards development remains part of the approved standard. CIP-013-1 Requirement R1 Part 1.2.6 addresses procurement processes related to vendor remote access. The proposed requirements in CIP-005-6 are operational in nature and not related to procurement. Therefore the requirements are not duplicative. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Request more guidance for the term "vendor" and use cases. If "Vendor" is not defined by NERC, the guidance should prompt Entities to include their definition of "vendor" in their plan(s). Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5	

Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.

The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard.

The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.

Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
As currently written, it is ambiguous in 2.4 as to why an entity needs to "determine" vendor access, especially in conjunction with the logging, monitoring and control activities described within the measures. PJM suggests combining 2.4 and 2.5 together ("Have one or more method(s) to determine and disable active vendor remote access sessions…").	
Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT believes parts 2.4 and 2.5 describe two distinct reliability objectives which should remain separate for clarity.	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
ITC Holdings agrees with the below comment submitted by MRO's NSRF: The NSRF question the use of "…*active* vendor…" in part 2.4 and 2.5 Requirements. The word "active" could mean either "the vendor is currently allowed electronic access and is currently within a BES Cyber Asset" OR "the vendor is idle and but has electronic access to a BES Cyber Asset". The NSRF recommends that "active" be removed as this will provide clarity to applicable entities. If active sessions was the SDT thought process, please state that within the proposed part.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT's intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. Meeting this objective does not require monitoring of remote access sessions in real time. The examples of evidence included in the Measures for Part 2.4 indicate that this method does not require monitoring of individual remote access sessions with a vendor in real time. Examples listed in the measure include: • *Methods for accessing logged or monitoring information to determine active vendor remote access sessions;* • *Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or* • *Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.*	

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

The definition of vendor is crucial to an entity defining and carrying out its compliance objectives for the requirements in question.

The definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-013.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Regarding CIP-005-6, R2.4 & R2.5; NRG requests that the NERC SDT define or further clarify the meaning of “system-to-system” remote access.

NRG asserts that Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Please include a reference to FERC Order 829 for Parts 2.4 and 2.5.

Please consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.

Requirement R2 Parts 2.4 and 2.5 address controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to “user-initiated access by a person”, the SDT included system-to-system remote access with a vendor(s) in the

requirement to meet the directive in Order No. 829 (P. 45). The SDT has clarified in rationale that the phrase *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i) is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (ii) is not IRA, and (iii) occurs between the Responsible Entity and a vendor. The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard.	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Does system to system remote access include “read-only” access or all forms of external access from vendors?	

Likes 0	
Dislikes 0	
Response. Thank you for your comments. Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all remote access sessions with vendors. This includes 'read-only' access.	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC supports NRECA's Comments of: NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has added clarification to the Rationale section. The rationale remains in the standard following approval.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

The proposed CIP-005-6 uses vendor. Definition of vendor is not a NERC defined term. USI believes the SDT should provide guidance regarding the use of the term "vendor." If "Vendor" is not defined by NERC, the Guidance should recommend that Entities include their definition of "vendor" in their plan(s). The SDT should consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5	
Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	
Response. Thank you for your comment. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard. The SDT does not believe a CIP Exceptional Circumstance would prevent an entity from having methods for determining active remote access sessions or disabling remote access sessions.	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
As stated, this requirement seems to start with the base assumption that the Registered Entity allows vendors to have Remote Access to the Registered Entity's BES Cyber Assets with External Routable Connectivity (ERC), and therefore must implement a method to detect active vendor remote access session and have a method for disabling vendor access. Many Registered Entities do not allow vendors to have Remote Access to substation medium BES Cyber Assets. Would this relieve such REs from having to then develop a method to detect and disable active vendor remote access session and would documentation demonstrating that Vendor Remote Access was not allowed be sufficient?	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. It is not the intent of the SDT to require entities to have documented processes for remote access if the entity does not allow remote access. The SDT has added clarification to the rationale section. The rationale remains in the standard following approval.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. It is not the intent of the SDT to require entities to have documented processes for remote access if the entity does not allow remote access. The SDT has added clarification to the rationale section. The rationale remains in the standard following approval.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
The definition of “vendor” is important for defining and carrying out its compliance objectives for the requirements parts 2.4 and 2.5. The drafting team should add a part of one or both requirements to include a specific definition of vendor to support the related compliance procedures and evidence required of an entity.	

For Part 2.4, it is not clear if the requirement applies to contractors and service vendors that are provided authorized access under CIP-004. Additionally, more information is needed on the meaning of "active". Most of this is captured in logs after the fact. Does the drafting team intend for "active" to imply real-time information? Please clarify if the requirement only applies to a connection from the vendor directly to a system within the ESP or does it apply to connections from a vendor to a system outside the ESP that updates one inside the ESP. For Part 2.5, Oncor would like clarification of the action, or examples, for when access should be disabled.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.

Part 2.4 does not exclude contractors and service vendors that are provided access under CIP-004. Parts 2.4 and 2.5 are intended to mitigate risks of a compromise at a vendor from traversing over a network connection and impacting BES Cyber Systems (Order No. 829 P. 52). Depending on the responsible entity's arrangements, contractor and/or vendor management of a Responsible Entity's BES Cyber System may not be within the scope of Parts 2.4 and 2.5. These requirement parts apply to Interactive Remote Access with a vendor and system-to-system remote access with a vendor. The SDT has clarified in rationale that the phrase *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i) is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (ii) is not IRA, and (iii) occurs between the Responsible Entity and a vendor.

The SDT's intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. Meeting this objective does not require monitoring of remote access sessions in real time. The examples of evidence included in the Measures for Part 2.4 indicate that this method does not require monitoring of individual remote access sessions with a vendor in real time. Examples listed in the measure include:

- *Methods for accessing logged or monitoring information to determine active vendor remote access sessions;*

- *Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or*
- *Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.*

CIP-005-6 Requirement R1 Part 1.5 could provide a mechanism for Responsible Entities to determine when a response to suspicious activity in a vendor remote access session may be warranted. Part 1.5 requires Responsible Entities to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. Detections associated with this requirement could determine when a responsible entity should disable vendor remote access.

Lona Calderon - Salt River Project - 1,3,5,6 – WECC	
Answer	Yes
Document Name	
Comment	

SRP agrees with R2 Part 2.4 but requests clarification of the term “determining.”

SRP generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective “…is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. SRP requests changing the language to “upon detected unauthorized activity.”

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective. The SDT has revised the rationale and removed the subjective term 'rapidly'. The objective of part 2.5 is for entities to have the ability to disable active remote access sessions.

Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	

Request to defined the scope of the requirements "for new contracts only"

With no defined scope, if the standard become effective in same time of the standard CIP-013-1, no terms will existed beetween entities and vendor in effective contracts. How the entities will comply to requirements ?

Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005.

Request more guidance for the term "active vendor remote access sessions" and use cases. Guidance should prompt Entities to include their definition of "vendor" in their plan(s).

Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5

Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT does not agree with limiting the scope to new contracts. The SDT believes responsible entities can and should meet the requirements upon implementation of the standard. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard. *Active* sessions refers to remote access sessions with vendors that are taking place on the responsible entity's system at any point in time. The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See atttached comments.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.	

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective. The SDT has revised the rationale and removed the term 'rapidly'. The objective of part 2.5 is for entities to have the ability to disable active remote access sessions. The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro sees value in adding the machine to machine vendor remote access component.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes

Document Name	
Comment	
AE agrees with R2 Part 2.4 but requests clarification of the term “determining.” AE generally agrees with Proposed R2 Part 2.5, but requests revisions to the rationale for R2. The last sentence of paragraph 2 states the objective “is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. AE requests changing the language to “upon detected unauthorized activity.”	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective. The SDT has revised the rationale and removed the subjective term ‘rapidly’. The objective of part 2.5 is for entities to have the ability to disable active remote access sessions.	
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 with R2 Part 2.4 but requests clarification of the term “determining.” SMUD generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective “is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. SMUD requests changing the language to “upon detected unauthorized activity.” Clarification or formal definition of the term ‘vendor’ should be considered. ICCP and DNP3 traffic is routine system-to-system remote access between utilities, Operation and Maintenance vendors and other partners to provide reliability, without the term ‘vendor’ clarified, these protocols may fall into scope unnecessarily.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective. The SDT has revised the rationale and removed the subjective term ‘rapidly’. The objective of part 2.5 is for entities to have the ability to disable active remote access sessions. Parts 2.4 and 2.5 are intended to mitigate risks of a compromise at a vendor from traversing over a network connection and impacting BES Cyber Systems (Order No. 829 P. 52). As stated in the rationale, NERC registered entities are not considered vendors within the scope of the requirements. The SDT did not intend to exclude certain remote access on the basis of a responsible entity considering the remote access to be ‘routine’.	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	

Comment
PRPA agrees with R2 Part 2.4 but requests clarification of the term “determining.” PRPA generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective “is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. PRPA requests changing the language to “upon detected unauthorized activity.”

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective.

The SDT has revised the rationale and removed the subjective term ‘rapidly’. The objective of part 2.5 is for entities to have the ability to disable active remote access sessions.

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment
ReliabilityFirst agrees the changes to CIP-005-6 address directives from Federal Energy Regulatory Commission (FERC) Order No. 829 to develop a new or modified standard to address “supply chain risk management for industrial control system hardware, software, and

computing and networking services associated with bulk electric system operations." ReliabilityFirst offers the following specific comments for consideration.

1. Requirement R2 Part 2.3
    i. To be consistent with Parts 2.1 and 2.2 in the Standard, ReliabilityFirst offers the following modifications for consideration:
        a. [For all Interactive Remote Access sessions, require] multi-factor authentication.
2. Requirement R2 Part 2.4
    i. ReliabilityFirst believes more context should be placed around the term "determining". ReliabilityFirst offers the following modifications for consideration:
        a. Have one or more method(s) for [authorizing, monitoring, and logging] active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT believes part 2.3 is clear as written.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective. The SDT believes the suggested wording could create overlapping obligations with some approved CIP requirements. The SDT prefers the drafted wording because it provides responsible entities with more flexibility to meet the objective.

Allan Long - Memphis Light, Gas and Water Division - 1

Answer	Yes
Document Name	
Comment	
Because the term "vendor" is not a NERC-defined term, the SDT should provide guidance regarding its use. A "CIP Exceptional Circumstance" clause should be added to R2, Parts 2.4 and 2.5.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard. The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
A definition of “vendor” is necessary. This should be interpreted as any third-party that initiates a remote access session. Not every third-party is necessarily considered a “vendor” based on generally accepted definitions. With respect to the proposed Requirement 2 Part 2.4, additional details need to be provided on the expectations of “determining active vendor remote access sessions”. Two of the proposed measures state, “Methods for monitoring activity (e.g. connection tables or rule hit	

counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; **or** Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access." The former will be difficult to actively monitor for remote access. Remote access can be monitored, but this activity is too resource intensive to monitor in real-time. If it is necessary to actively monitor remote access in real-time then additional guidance is necessary. The latter is easily implemented. It is uncertain whether this requirement is expecting constant monitoring during the remote access session or just controlling access and logging the access. A more detailed expectation on the use of the reference tools is necessary.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard. Some remote access, such as between NERC Registered Entities, is not considered in scope for Parts 2.4 and 2.5. The SDT's intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. Meeting this objective does not require monitoring of remote access sessions in real time. However, a responsible entity could choose to monitor vendor remote access sessions in real time as a way to meet its obligation in Part 2.4.	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	Yes
Document Name	
Comment	

No comment.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
As in Question 1, regarding the use of the term “vendor,” as described in the “Rationale for Requirement R2” section of CIP-005-6: the SDT may want to clarify that staff augmentation contractors are not considered to be “vendors” in the context of the standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. Parts 2.4 and 2.5 are intended to mitigate risks of a compromise at a vendor from traversing over a network connection and impacting BES Cyber Systems (Order No. 829 P. 52). Depending on the responsible entity’s arrangements, staff augmentation contractors may not be within the scope of Parts 2.4 and 2.5. These requirement parts apply to Interactive Remote Access with a vendor and system-to-system remote access with a vendor.	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	

Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
We request clarification 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, or whether the SDT intent is that any system-to-system access be included. We would suggest that the SDT add verbiage to the Guidelines and Technical Basis making the distinction for each type of “active vendor remote access sessions” that are included in this requirement (Interactive Remote Access, system-to-system remote access with control, and/or system-to-system remote access for monitoring only). Another suggestion would be to create a formal NERC definition of system-to-system access.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Parts 1.2.6 addresses controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to “user-initiated access by a person”, the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45). The controls specified in Part 1.2.6 cover all remote access with vendors, which includes one-way remote access. System to system remote access is any remote access that: (i) is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor.

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
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	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 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	

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
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	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
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	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	

Document Name	
Comment	
Please clarify definition of system-system communications	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has clarified in rationale that the phrase *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i) is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (ii) is not IRA, and (iii) occurs between the Responsible Entity and a vendor.	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	

Document Name	
Comment	
The NSRF question the use of "…*active* vendor…" in part 2.4 and 2.5 Requirements. The word "active" could mean either "the vendor is currently allowed electronic access and is currently within a BES Cyber Asset" OR "the vendor is idle and but has electronic access to a BES Cyber Asset". The NSRF recommends that "active" be removed as this will provide clarity to applicable entities. If active sessions was the SDT thought process, please state that within the proposed part.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT's intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. Meeting this objective does not require monitoring of remote access sessions in real time. The examples of evidence included in the Measures for Part 2.4 indicate that this method does not require monitoring of individual remote access sessions with a vendor in real time. Examples listed in the measure include:

- *Methods for accessing logged or monitoring information to determine active vendor remote access sessions;*
- *Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or*
- *Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.*

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 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). The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Disagree with the revisions on CIP-010-3, would like to see guideline language of verifying once be moved to the requirement/measure	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. SDT added guidance to support use of software repositories so that verification checks are not duplicated for each installation. The SDT believes the requirement and measures are worded to provide responsible entities flexibility to use this approach.	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
Need additional information regarding how to verify integrity of software.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has added information to the guidelines section.	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests additional guidance as to what constitutes acceptable verification of integrity as required by R1.6.2. The measure indicates that a change request record could demonstrate that source identity and integrity verification took place, but doesn't go into further detail as to what an acceptable check into source identity and software would be. Is there specific language that should be stated in the change request record that would clearly state the verification took place? More guidance on this aspect is requested. Also, Duke Energy requests that the Note under Applicable Systems in Part 1.6 should remain there once the standard is approved. The Note provides valuable details as to the true scope of the Requirement, and aids entities in knowing what will be the compliance expectation.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has added information to the guidelines section. The note remains in the Part 1.6 when the standard is approved.	
Timothy Reyher - Eversource Energy - 5	
Answer	No

Document Name	
Comment	

Comments:

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

VSL does not cover the failure to implement the process. Does not include all of the combinations.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence

We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions:

How does one prove that a method is not available?

What is the line between available/unavailable? How far do you have to go?

We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. Additional examples are included.

For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1.

An entity could demonstrate that a method to verify integrity is not available by providing documentation from the software source that shows the method to verify integrity is not provided, could provide evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation.

The SDT included 'when a method to do so is available' to provide flexibility necessary to prevent disruption of an entity's software update and patch management processes. Part 1.6 does not impact an entity's ability and obligation to meet CIP-007 R2.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

VSL does not cover the failure to implement the process. Does not include all of the combinations.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence

We suggest rephrasing "when the method to do so is available to the Responsible Entity from the software source" to "when the vendor supplied method to do so is available to Responsible Entity". Otherwise the "method to do so" is ambiguous and leaves the following questions:

How does one prove that a method is not available? What is the line between available/unavailable? How far do you have to go? We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response. Thank you for your comments. SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. Additional examples are included. For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1. An entity could demonstrate that a method to verify integrity is not available by providing documentation from the software source that shows the method to verify integrity is not provided, could provide evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. The SDT included 'when a method to do so is available' to provide flexibility necessary to prevent disruption of an entity's software update and patch management processes. Part 1.6 does not impact an entity's ability and obligation to meet CIP-007 R2.	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	

Comment	
The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation.	
IESO	
Answer	No
Document Name	
Comment	
The IESO is concerned with two aspects of CIP-010-3 Requirement R1 Part 1.6: 1. The phrase “when the method to do so is available to the Responsible Entity from the software source” will be difficult to audit and difficult for the Responsible Entity to confirm as it is hard to prove a negative. The IESO suggest that verification of software source and integrity can take many different forms and is a sufficiently common practice that this phrase is not required. To take into consideration legacy software, the IESO suggest the wording be adjusted, to reflect FERC intentions that the requirements are forward looking, by replacing the phrase “and when the method to do so is available to the Responsible Entity from the software source” with “and, at a minimum, for the portion of the software that has changed:”	

2. There appears to be inconsistency between the requirement and the Guidelines.

The requirement states “For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5”.

The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

The requirement wording suggests it applies for any change but the guidance suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the guidance is not, the guidance becomes superfluous. The Guideline also introduces significant ambiguity that is impossible to audit.

Therefor the IESO suggest that either the requirement wording be adjusted to allow for automated patching solutions or the Guideline be removed as it is contradictory. The IESO suggest that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore the best solution is to remove the guideline.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

SDT believes the phrase ‘when a method to do so is available’ provides responsible entities with necessary flexibility to perform configuration management obligations. Responsible entities have varying baselines, software vintages, and vendor support. Flexibility may be needed to prevent disruption of an entity’s software update and patch management processes.

The SDT has removed unclear statements from the guidelines section and added additional guidance.

The SDT revised the measure for Part 1.6 to provide an example of evidence to support automated solutions.

William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
See attached integrated comments. (Comment at end of document)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
To avoid an interpretation of this requirement that may be overly burdensome, ERCOT suggests the following clarifications to the language in the requirement and measure of CIP-010-3 R1 Part 1.6. This would ensure a more holistic and less prescriptive approach to changes that deviate from the baseline. In the first sentence of Requirement R1.6, revise "For a change that deviates" to "Where technically feasible, for changes that deviate…" Revise the R1.6 Measure to read "An example of evidence may include, but is not limited to, a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed during the baseline change, *or a process which documents the mechanisms in place that would automatically ensure the authenticity and integrity of the software."*	
Likes 0	

Dislikes 0	
Response. Thank you for your comments. The SDT included the wording 'when a method to do so is available', which is intended to cover issues that would include technical feasibility. The SDT has made the suggested change to the measure for Part 1.6.	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD believes the R1.6 "Note:" within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; "CHPD has concerns about language related to procurement contracts, in particular use of master agreements,	

piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013.” CIP-010 R1.6 – Applicable System Note *“Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.”*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the note is consistent with the forward-looking nature of Order No. 829. The SDT also believes Part 1.6 is performance-based.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD believes the R1.6 “Note:” within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; “CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013.” CIP-010 R1.6 – Applicable System Note	

"Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract."	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the note is consistent with the forward-looking nature of Order No. 829. The SDT also believes Part 1.6 is performance-based.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD believes the R1.6 "Note:" within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; "CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to "contracts" and most references to "procurement" be struck from CIP-013." CIP-010 R1.6 – Applicable System Note *"Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract."*	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT believes the note is consistent with the forward-looking nature of Order No. 829. The SDT also believes Part 1.6 is performance-based.	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD believes the R1.6 "Note:" within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; "CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to "contracts" and most references to "procurement" be struck from CIP-013." CIP-010 R1.6 – Applicable System Note *"Note: Implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract."*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the note is consistent with the forward-looking nature of Order No. 829. The SDT also believes Part 1.6 is performance-based.	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	No
Document Name	

Comment
The language should make clear that verification is required for the software intake process, but not for each subsequent installation. We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions: - How does one prove that a method is not available? - What is the line between available/unavailable? How far do you have to go? We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.
Likes 0
Dislikes 0
Response. Thank you for your comments. The SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. Part 1.6 provides responsible entities with flexibility to meet the reliability objective. A responsible entity could use a verification method that is provided by the vendor, or another method that is available. Techniques described in the guidelines and technical basis section are not limited to those provided by the software’s vendor. An entity could demonstrate that a method to perform verification is not available by providing documentation from the software source, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. The SDT included ‘when a method to do so is available’ to provide flexibility necessary to prevent disruption of an entity’s software update and patch management processes. Part 1.6 does not impact an entity’s ability and obligation to meet CIP-007 R2.
Shawn Abrams - Santee Cooper - 1

Answer	No
Document Name	
Comment	

Need clarification about how the addition of R1.6 applies only to BES Cyber Systems that are newly implemented and thus did not previously have a baseline and as such do not have an existing baseline to deviate from. Please clarify that this is for new BES Cyber Systems to avoid confusion and challenges during an aduit.

Need some additional examples of what constitutes evidence to meet compliance to this standard. Some systems are not connected to the internet purposefully and as such patches are installed utilizing a CD/DVD provided by the vendor. What would constitute appropriate evidence for a case such as this?

This requirement is not clear whether an entity has to duplicate efforts for every case for which such verification has to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that an entity can verify once and apply to many assets.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is “intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System” (P. 49). Performing software verifications as part of establishing the baseline is not in scope for Part 1.6. Baseline changes to the responsible entity’s high impact and medium impact BES Cyber Systems after the effective date of proposed CIP-010-3 are in scope (i.e., Part 1.6 is not limited to new BES Cyber Systems.)

SDT has provided additional technical considerations and examples in the guidance section, and revised the measure. SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation.

Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
Since the intent of CIP-010-3 R1.6 is a proactive verification of software integrity, R1.6 should focus on a single verification prior to introducing vendor software into the production environment. The current language of R1.6 utilizes a retroactive focus via baseline deviations. Please see the suggested wording - "Prior to introducing software not resident in baseline items (per 1.1.1, 1.1.2, and 1.1.5), and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source."	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has revised Part 1.6 to clarify that the verifications are to be performed prior to the baseline change.	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

Proposed Requirement R1 Part 1.6 appears to require verification of identity and integrity of applicable changes to the baseline. However, the measure for this requirement gives an example of having a process, e.g., a change request record, instead of a specific example of verification. Can the team clarify the measure for this Requirement as an entity can have a change ticket process that merely requires the user to click a button that states that the software has been verified, however, if the team believes proof of such check, such as a screenshot of the vendor site, is required, please state such as an example. Additionally, the example of evidence does not demonstrate how a software source or the software integrity is verified. An internal change ticket is not a verification of the software source. If they are going to push for source verification then modify CIP-007 R2.1 to include it. Specifically, what is expected as evidence -- a hash, screenshot, attestation, digital signature?	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has provided additional guidance and examples in the guidelines and technical basis section.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Even though ReliabilityFirst believes the changes to CIP-010-3 draft standard address directives from Federal Energy Regulatory Commission (FERC) Order No. 829 and is a positive step in addressing cyber supply chain management, ReliabilityFirst Abstains mainly due to Requirement R1 missing Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following specific comments for consideration. 1. Requirement R1 Part 1.6 2.	

i. ReliabilityFirst believes the "Applicable Systems" under Requirement R1 Part 1.6 should be consistent with "Applicable Systems" under parts 1.1, since sub-parts (Part 1.1.1, 1.1.2, & 1.1.5) are called out under the "Requirements" section for Part 1.6. EACMs and PACS are critical cyber assets that control access and monitoring into the entities' ESPs and PSPs and should follow the Supply Chain standard/requirements as do the High and Medium Impact Cyber Systems. As for the PCAs, if they are compromised due to a vulnerability in the vendors supplied hardware or software, they can possibly affect high and medium impact BES Cyber Systems. ReliabilityFirst offers the following modifications for consideration for the "Applicable Systems" column in Requirement R1 Part 1.6:

   a. High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA

   b. Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA

3. Requirement R1 Part 1.6.3 (new sub-part)

   i. ReliabilityFirst believes a new sub-part 1.6.3 should be added to address the verification of the baseline configuration. ReliabilityFirst offers the following new sub-part 1.6.3 for consideration:

      a. Verify the deviations from the baseline configuration.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT believes that Part 1.6 provides the intended reliability benefit, which applies to "industrial control system hardware, software, and services associated with bulk electric system operations" as specified in Order No. 829 (P. 43). The SDT believes entities should have flexibility to determine supply chain cyber security risk management controls for other cyber assets, including EACMS, PACS, and PCAs. The SDT believes this is an appropriate risk-based approach that allows entities to focus resources where they provide the most reliability benefit.

SDT believes there is reliability benefit to addressing the software integrity for changes from baseline configuration and that the requirement meets the directives in Order No. 829. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Verification of the integrity of the baseline configuration is not in scope.	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro does not agree with value-add of this standard requirement. Under current CIP requirements, CIP controls around testing of changes and ongoing monitoring of systems would mitigate any risk associated with software identity or integrity.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (Order No. 829 P. 49). The SDT agrees that other entity processes help mitigate risk. However, Part 1.6 is responsive to the project SAR and provides reliability benefit by addressing some verifications that are not covered under other standards.	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	

Ther is nothing wrong with the concept of the requiment however the language of the requirement is not supportable. The term available could me technically available, procedurally available, contracturaly available, freely available (no support purchase required). As written this requirement by its nature will be implemented and assessed drastically differently by different Responsible Entities. One could argue that only if all the available methods listed above exist in unison is software actually available.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. SDT has provided additional information in the guidance section. *Available from the software source* is not intended to be limited to contract terms. The SDT believes this wording is necessary to provide entities with flexibility and avoid disrupting software update and patch management processes in some situations.	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
There are auditing challenges around the phrase “when the method to do so is available to the Responsible Entity from the software source” as it is hard to prove a negative. Oncor believes that verification of software source and integrity can take many forms. To take into consideration legacy software, Oncor believes the wording should be adjusted, to reflect FERC intentions that the requirements are forward looking, by replacing the phrase *“and when the method to do so is available to the Responsible Entity from the software source”* with *“and, at a minimum, for the portion of the software that has changed:”* Second, the proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). We offer a recommendation on the language, *“Document and implement a software source management process to address source identity*	

verification and media integrity controls on the software repository used for changes that deviate from the existing baseline configuration associated with items in parts 1.1.1, 1.1.2, and 1.1.5." *This process must include steps:* *• To verify the identity of the software source when the method to do so is available; and* *• To verify the integrity of the software obtained when the method to do so is available.* *Evidence may include verification of identity of the software source and integrity of the software was performed for repository updates."*	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. An entity could demonstrate that a method to perform verifications is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). The SDT does not believe the replacement phrase for 'when a method to do so…" is necessary or provides additional clarity. Performing software verifications as part of establishing the baseline is not in scope for Part 1.6. SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. The SDT believes this addresses concerns with duplicating efforts.	
Don Schmit - Nebraska Public Power District - 5	
Answer	No

Document Name	
Comment	
NPPD supports the comments of the MRO NSRF, in addition: Auditors will have too much discretion as to what is or is not enough for a validation check of each vendor, which will lead to inconsistencies across the NERC RE footprint. It is up to entities to document what the vendor is willing to do and hope the auditors agree it is enough to continue doing business with the vendor. Also, the language of the requirement says "…when the method to do so is available…". If a vendor does not have a method to do so, but does in the next year or so, the entity may have a possible violation if it did not realize there was a change in the vendor's available methods. This would force entities to periodically check to see if the vendor capabilities have changed. What is the period that would not make this a violation? The requirement is very vague.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes Part 1.6 addresses the reliability objective for software verification contained in the project SAR and provides responsible entities with the flexibility necessary to meet the obligation. Responsible entities have varying baselines, software vintages, and vendor support. Flexibility may be needed to prevent disruption of an entity's software update and patch management processes. SDT has added guidance in the technical guidelines section to support responsible entities in adding this objective to their configuration change management processes.	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	

As currently written, "verify the identity" is too vague. PJM suggests adding examples of "identify" into the measure. PJM also suggests removing the word "software" from 1.6.1 and 1.6.2 as it is already stated within parts 1.1.1, 1.1.2 and 1.1.5 (firmware should be within the scope of 1.6).	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT added guidance in the guidelines section of the standard. The scope of Part 1.6 includes any changes (software or firmware) in 1.1.1, 1.1.2, and 1.1.5.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many. Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence. We support these changes, but requests clarification about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.	
Likes 0	

Dislikes 0	

Response. Thank you for your comments.

The SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. Technical considerations and examples associated with Part 1.6.1 and Part 1.6.2 are included.

Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Performing software verifications as part of establishing the baseline (e.g., implementing a new BES Cyber System) is not in scope for Part 1.6.

Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	

Comment

Request clarification on how an Entity can verify the 'integrity and authenticity' one time and then be able to install on multiple devices.

Recommend removing CIP-013 R1 subparts 1.2.5 from CIP-013 since it is covered in the proposed CIP-010-3

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

VSL does not cover the failure to implement the process. Does not include all of the combinations.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence

We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions: How does one prove that a method is not available? What is the line between available/unavailable? How far do you have to go? We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. Technical considerations and examples associated with Part 1.6.1 and Part 1.6.2 are included.

CIP-013-1 Requirement R1 Part 1.2.5 addresses procurement processes related to software verification. The proposed requirement in CIP-010-3 is operational in nature and not related to procurement. Therefore the CIP-013 requirement is not duplicative of the CIP-010-3 requirement. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1.

Part 1.6 provides responsible entities with flexibility to meet the reliability objective. A responsible entity could use a verification method that is provided by the vendor, or another method that is available. Techniques described in the guidelines and technical basis section are not limited to those provided by the software’s vendor. An entity could demonstrate that a method to perform verification is not

available by providing documentation from the software source, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. The SDT included 'when a method to do so is available' to provide flexibility necessary to prevent disruption of an entity's software update and patch management processes. Part 1.6 does not impact an entity's ability and obligation to meet CIP-007 R2.	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
To ensure that resources are appropriately focused on changes to be applied, AZPS recommends clarifying that verification should be completed "prior to application of a change." Such a clarification will signal to entities that verification only needs to be performed where a change will be applied and avoid circumstances where a change is being evaluated for application and verification occurs, but the change is not applied. Under the current obligation, it is likely that verifications and associated evidence would be prepared regardless of whether the change is or is not applied and would therefore result in the dedication of resources to efforts that would have no benefit to reliability or security. Additionally, AZPS requests clarification regarding the continued need for verification evidence where such is not available from the vendor. Specifically, AZPS notes that, where a vendor's policy does not provide the necessary evidence associated with verification, this Requirement may frequently represent null evidence for areas where items are reviewed each time a change occurs, but no data is available due to the vendor's policies. Such efforts would be redundant and of little or no value to security and reliability.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has revised Part 1.6 to clarify that the verifications are to be performed prior to the baseline change.	

The SDT believes Part 1.6 and its associated measure provide the responsible entity with flexibility to develop configuration change management processes and evidence that minimize redundant efforts. Specific questions pertaining to auditing and compliance are not in scope for the SDT.	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Add language to address CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT discussed the suggestion to add CIP Exceptional Circumstance and did not believe this was necessary for reliability. The SDT believes the steps for verifications, when methods are available, can be implemented in emergent and non-emergent scenarios. Furthermore, responsible entities are not obligated to perform verifications when a method to perform the verifications is not available.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	

Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
GRE and NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: "For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer." This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the guidelines section to address this issue.	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG suggest that 1.6.1 state "Verify the software originated from the vendor's official source(s)". In the current text, even if a source has an "identity", it should also state the "identity" is the one that is expected. Similarly we can change the word "identity" with "correct identity" in R1 Part 1.6.1.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. SDT agrees that verifying identity of source means that the software is being obtained from the correct source. The SDT believes the additional information provided in the guidance section clarify the intent.	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
By adding the "when the method to do so is available to the Entity from the software source" does this require the entity to document and detail what method is available of not available? How does that entity prove and document this condition? Does the entity have to document and prove that it was tested and verified for software integrity and authenticity? If so, what are those requirements, documentation, testing environment required and timeline for testing the software?	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation.	
Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	

AECI supports NRECA's comments provided below: NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: "For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer." This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the guidelines section to address this issue.	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
GTC supports NRECA comments: NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: "For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer." This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the guidelines section to address this issue.	
Victor Garzon - El Paso Electric Company - 5	

Answer	Yes
Document Name	
Comment	

EPE understands the need for software integrity and authenticity; however, the proposed wording of the standard is not sufficiently clear with respect to the action/conduct being sought by the Registered Entity in order to achieve compliance. In Order No. 829, FERC offered clarity that the proposed requirement does not capture. There, FERC stated:

For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and components should be tested and verified using controls such as digital signatures and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without **verification that the component has been digitally signed** to ensure that hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides **examples of controls for addressing the Commission's directive regarding this first objective. Other security controls also could meet this objective.** Order No 829 at P 50 (emphasis added).

Requirement 1.6 should be adjusted to provide the type of clarity FERC provided in the Order. An additional sentence or parenthetical should be included within the requirement, to read ("Verification that a patch or other software component has been digitally signed is one way to meet this requirement; other security controls could also meet this requirement, such as having the vendor state in writing that it will verify the integrity and authenticity of all software, including patches, in advance of releasing it to the Registered Entity during the life of its service contract with the Registered Entity").

The addition of such language *in the requirement itself* is consistent with the feedback offered by NERC Staff in recent months, and would eliminate the false impression that would otherwise be given that a Registered Entity must secure a verification letter from its software vendor each and every single time it seeks to download a patch. For example, during the NERC webinar held on May 18, 2017, examples were provided to the attendees on information that would be considered sufficient evidence to fulfill this requirement, and such examples included a letter from the vendor indicating that the vendor is verifying integrity and authenticity of its software before releasing its software (including patches) to its clients.

Likes 0	

Dislikes 0	
Response. Thank you for your comment. Consistent with other NERC Reliability Standards, the suggested clarifications are more appropriately addressed in the guidelines section of the standard. The SDT has added details to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard.	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	

EPE understands the need for software integrity and authenticity; however, the proposed wording of the standard is not sufficiently clear with respect to the action/conduct being sought by the Registered Entity in order to achieve compliance. In Order No. 829, FERC offered clarity that the proposed requirement does not capture. There, FERC stated:

For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and components should be tested and verified using controls such as digital signatures and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without **verification that the component has been digitally signed** to ensure that hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides **examples of controls for addressing the Commission's directive regarding this first objective. Other security controls also could meet this objective.** Order No 829 at P 50 (emphasis added).

Requirement 1.6 should be adjusted to provide the type of clarity FERC provided in the Order. An additional sentence or parenthetical should be included within the requirement, to read ("Verification that a patch or other software component has been digitally signed is one way to meet this requirement; other security controls could also meet this requirement, such as having the vendor state in writing that it will verify the integrity and authenticity of all software, including patches, in advance of releasing it to the Registered Entity during the life of its service contract with the Registered Entity").

The addition of such language *in the requirement itself* is consistent with the feedback offered by NERC Staff in recent months, and would eliminate the false impression that would otherwise be given that a Registered Entity must secure a verification letter from its software vendor each and every single time it seeks to download a patch. For example, during the NERC webinar held on May 18, 2017, examples were provided to the attendees on information that would be considered sufficient evidence to fulfill this requirement, and such examples included a letter from the vendor indicating that the vendor is verifying integrity and authenticity of its software before releasing its software (including patches) to its clients.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Consistent with other NERC Reliability Standards, the suggested clarifications are more appropriately addressed in the guidelines section of the standard. The SDT has added details to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard.	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
EPE understands the need for software integrity and authenticity; however, the proposed wording of the standard is not sufficiently clear with respect to the action/conduct being sought by the Registered Entity in order to achieve compliance. In Order No. 829, FERC offered clarity that the proposed requirement does not capture. There, FERC stated: *For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and components should be tested and verified using controls such as digital signatures and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without verification that the component has been digitally signed to ensure that hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing the*	

Commission's directive regarding this first objective. Other security controls also could meet this objective. Order No 829 at P 50 (emphasis added).

Requirement 1.6 should be adjusted to provide the type of clarity FERC provided in the Order. An additional sentence or parenthetical should be included within the requirement, to read ("Verification that a patch or other software component has been digitally signed is one way to meet this requirement; other security controls could also meet this requirement, such as having the vendor state in writing that it will verify the integrity and authenticity of all software, including patches, in advance of releasing it to the Registered Entity during the life of its service contract with the Registered Entity").

The addition of such language *in the requirement itself* is consistent with the feedback offered by NERC Staff in recent months, and would eliminate the false impression that would otherwise be given that a Registered Entity must secure a verification letter from its software vendor each and every single time it seeks to download a patch. For example, during the NERC webinar held on May 18, 2017, examples were provided to the attendees on information that would be considered sufficient evidence to fulfill this requirement, and such examples included a letter from the vendor indicating that the vendor is verifying integrity and authenticity of its software before releasing its software (including patches) to its clients.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. Consistent with other NERC Reliability Standards, the suggested clarifications are more appropriately addressed in the guidelines section of the standard. The SDT has added details to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard.

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Additional examples of acceptable evidence would be helpful under the Measures column of the requirement.

Change the statement in the Guidelines and Technical Basis, Section Software Integrity and Authenticity, paragraph 1, third sentence: "The intent of the SDT is to provide controls for verifying the baseline elements that are *updated* by vendors." to say "… *provided* by vendors." Additional clarity is needed regarding the following in the Guidelines and Technical Basis: "It is not the intent of the SDT to require a verification of each source *or software update at the time it is obtained*. It is sufficient to *establish the reliable source and software update once*. This will allow automated solutions to be implemented to obtain frequent updates such as patches." This is confusing because saying "each source or software update" is not required to be validated at the time it is obtained could be interpreted to mean continuous patch updates provided by a single vendor are only required to be verified once for the lifetime of the supply of patches from that vendor. Additional examples of acceptable methods and evidence are needed in the Guidelines and Technical Basis for performing software integrity and authenticity. For example – Consider having the measures for R1.6 be similar to R1.1.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT revised the Measure for Part 1.6 to more clearly include automated processes for verifications. The SDT has added details to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard. The SDT believes the suggested change of *updated* to *provided* could confuse some responsible entities because the requirement applies to baseline changes only; therefore the SDT does not support the wording change. SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. In doing so, the SDT removed ambiguous information from the guidelines section.
Teresa Cantwell - Lower Colorado River Authority - 1

Answer	Yes
Document Name	
Comment	
Disagree with the revisions on CIP-010-3. We would like to see guideline language of verifying once be moved to the requirement/measure.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. SDT added guidance to support use of software repositories so that verification checks are not duplicated for each installation. The SDT believes the requirement and measures are worded to provide responsible entities flexibility to use this approach.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	

Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes

Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	

Comment	
We request clarification on the timing of requirement 1.6; specifically, on whether 1.6 must be completed before being placed in operation on a BES Cyber System. This distinction was made in the previous draft ("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"). Under the current language, it appears sub-requirement 1.6 could be done before or after the software is placed on a BES Cyber System. We suggest the SDT add a timeframe similar to the other CIP-010 R1 sub-requirements. For example, 1.3 states "within 30 days" while 1.4.1 states "prior to the change". Additionally, we request adding 1.1.3 (any custom software installed) to 1.6, as custom software could be internally or externally provided, and needs to be verified for integrity and authenticity.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised Part 1.6 to clarify that the verifications are to be performed prior to the baseline change.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Rueckert - Western Electricity Coordinating Council - 10	

Answer	Yes
Document Name	
Comment	
No issues from an SCRM perspective. Part 1.6 is generic and can be considered a good idea for all changes from baseline configurations described in Parts 1.1.1, 1.1.2, and 1.1.5.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	

Comment
Need to emphasize the phrase “and when the method to do so is available to the Responsible Entity for the software source”. Since this is a non-prescriptive requirement it is expected that we will be demonstrating compliance by implementing the plan(s) required in CIP-013. Since it may not be possible to hold the software resource directly responsible it is expected that the demonstration of “best effort” will be sufficient and not subject to interpretation by the Compliance Enforcement Authority. Recommend providing more examples of suitable evidence that should be gathered to verify identity and integrity. The Measure as currently written is too vague.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT has added details to the guidelines section to provide technical considerations and examples that improve the clarity of the standard.

Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	

Comment
We support APPA's submitted comments, including: This requirement would possibly involve entitites duplicating effort for every case for which such verification had to be undertaken. More examples of evidence should be provided. Clarification is needed about how new R1.6 applies to entirely new BES Cyber Systems.

Likes 0	

Dislikes 0	

Response. Thank you for your comment.

SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard.

Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.

Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	

PRPA agrees this requirement belongs in CIP-010 R1. PRPA generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- PRPA recommends the Guidelines and Technical Basis section is updated to reflect current information.
    - The requirement states "For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5…," indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: "It is not the intent of the SDT to require a

verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."

- PRPA also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.

- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed. Additionally, PRPA requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While PRPA supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written.

An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is “intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System” (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
The Guidelines and Technical Basis of CIP-010-3 states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.” CenterPoint Energy recommends incorporating this concept in the R2 requirement language in order to clarify that integrity and authenticity do not need to be verified for every source or software update, and that the download once and install on many approach is acceptable if the integrity and authenticity of the downloaded software are validated. CenterPoint Energy recommends adding the following language to Requirement R2: Upon validation of the integrity and authenticity of software, a Responsible Entity does not need to verify the integrity and authenticity for subsequent updates of such software.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT is addressing this concern by adding guidance to the guidelines section that supports use of software repositories so that integrity checks are not duplicated for each installation.
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 this requirement belongs in CIP-010 R1. SMUD generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- SMUD recommends the Guidelines and Technical Basis section is updated to reflect current information.
    -
        - The requirement states “For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5…,” indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

- SMUD also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.

- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed. Additionally, SMUD requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While SMUD supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

•

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written.

An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.

Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	

AE agrees this requirement belongs in CIP-010 R1 and generally agrees with Proposed R1 Part 1.6, but request the SDT address the following items:

AE recommends the Guidelines and Technical Basis section be updated to reflect current information.

The requirement states "For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5…," indicating the authenticity and integrity of the specified parts must be verified each time a baseline changes for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to occur (e.g., in the cases of multiple installations of software across many applicable Cyber Assets). This requirement does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe the existing statement in the GTB provides clarity on this issue and request it not be removed. From the GTB: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."

o AE also recommends rewording the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work. o There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system. o Additional examples of acceptable measures should to be listed. Additionally, AE requests examples of acceptable evidence when there is no method available to verify the identity of the software source. While AE supports these changes, clarification is required about how R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS newly implemented and which have no previous baseline, and thus do not have an existing baseline from which a change can occur. We expect R1.6 is intended to apply to new BCS as well as to existing BCS but, as written, the requirement does not. Please clarify to avoid implementation confusion and audit challenges.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written. An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation.	

Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is “intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System” (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx

Comment
See attached comments

Likes 0	
Dislikes 0	

Response. Thank you for your comments. SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written. An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation.

Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
Request to defined the scope of the requirements "for new contracts only" With no defined scope, if the standard become effective in same time of the standard CIP-013-1, no terms will existed beetween entities and vendor for effective contracts. How the entities will be conformed to requirements ? The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. VSL does not cover the failure to implement the process. Does not include all of the combinations. Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

The SDT does not agree with limiting the scope to new contracts. The SDT believes responsible entities can and should meet the requirements upon implementation of the standard. SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written. For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1.

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SRP agrees this requirement belongs in CIP-010 R1. SRP generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- SRP recommends the Guidelines and Technical Basis section is updated to reflect current information.
    - The requirement states “For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5…,” indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present

an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."

- SRP also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.

- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed. Additionally, SRP requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While SRP supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible

entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written. An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	

Comment	
NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: "For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer." This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the guidelines section to address this issue.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST believes the "if you can, you must" qualifying language in this proposed requirement part should be added to at least some parts of CIP-013 R1 and R2.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT does not believe that it is necessary to include this phrase in CIP-013-1 Requirement R1 Part 1.2. because CIP-013-1 addresses the responsible entity's procurement processes. CIP-013 does not impose obligations on vendors, nor does it obligate the responsible entity to specific terms or conditions in a contract.	
David Rivera - New York Power Authority - 3	

Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The NSRF has the same comment from CIP-013-1 R1: CIP-010-3 R1.6 is troublesome as well. 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. Thank you for your comments. The SDT has revised the measure for Part 1.6 to include evidence of meeting the requirement using automated update mechanisms. The SDT has also added details to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard.	

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."

USI has concerns with R 1.6.1 and 1.6.2 as written about how to provide evidence? Therefore, we believe more examples of evidence should be provided.

While we support these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response Thank you for your comments.

SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible

entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written. Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is “intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System” (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC supports NRECA's Comments of: NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: “For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer.” This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the guidelines section to address this issue.	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	

Comment	
R1.6 brings to mind several challenges. The intent appears to be to ensure that software is validated, which is not the issue. The issue is the auditability of the requirement and its existing language. The wording "when the method to do so is available" puts additional obligations on the Responsible Entity to prove whether the methods were available or not, when the methods were available, if it was appropriate to utilize the available methods in a given circumstance. It adds additional nuance when the methods are often obtained from third parties. If it is a legacy contract and has not been updated and the method is available to other entities but not to the Responsible Entity due to the legacy contract, is the method considered available? The intent of this requirement is good but the auditability of the language is challenging at best and should be adjusted to consider how entities will be able to document and comply with the requirement language.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. SDT believes the phrase 'when a method to do so is available' provides responsible entities with necessary flexibility to perform configuration management obligations. Responsible entities have varying baselines, software vintages, and vendor support. Flexibility may be needed to prevent disruption of an entity's software update and patch management processes. The SDT added details to the guidelines section that provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard.	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
• Please provide clarification to what, "verification of identity of the software source and integrity of the software" means. Please provide more examples within the Measures to ensure entities are prepared for compliance oversight expectations.	
Likes 0	

Dislikes 0	
Response. Thank you for your comments. The SDT added details to the guidelines section that provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2. Additionally, the Measure was revised to include evidence of meeting the requirement using automated update mechanisms.	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
SPP recommends that the drafting team provide examples to provide clarity on control design to meet the intent of the standard.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT added details to the guidelines section that provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

NRG recommends that the drafting team provide examples to provide clarity on control design to meet the intent of the standard.

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. NRG requests guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

The VSL as currently written may not cover the failure to implement the process. The VSL may not include all of the combinations.

NRG has concerns with Parts: 1.6.1 and 1.6.2 as written --- For example, how would a Registered Entity be expected to provide evidence? NRG request additional examples of evidence in the Measures section of the requirement.

NRG suggests rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” may be ambiguous and leaving the following questions:

How does one prove that a method is not available?

What is the line between available/unavailable? How far do you have to go?

NRG is concerned with double jeopardy potential with CIP-007 R2. NRG is concerned that it may be difficult or impossible to validate the source or verify authenticity of the patch itself which may cause the industry to not consider that patch to be available.

Likes 0	
Dislikes 0	
Response Thank you for your comments. The SDT added details to the guidelines section that provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2. This includes guidance to support use of software repositories so that integrity checks are not duplicated for each installation. For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1. Part 1.6 provides responsible entities with flexibility to meet the reliability objective. A responsible entity could use a verification method that is provided by the vendor, or another method that is available. Techniques described in the guidelines and technical basis section are not limited to those provided by the software's vendor. An entity could demonstrate that a method to perform verification is not available by providing documentation from the software source, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. The SDT believes the phrase 'when a method to do so is available' provides responsible entities with the flexibility necessary to prevent disruption of their software update and patch management processes. Thus, Part 1.6 does not impact an entity's ability and obligation to meet CIP-007 R2.	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	

ITC Holdings believes the wording of CIP-010-3 leaves a lot of room for interpretation and needs to be more prescriptive. The measures should define technical examples (e.g., denote MD5 fingerprint or hashing as being an acceptable method). Additionally, ITC recommends including Remedy in the Technical Guidance document if you can't use the file integrity method.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes Part 1.6 addresses the reliability objective for software verification contained in the project SAR and provides responsible entities with the flexibility necessary to meet the obligation. Responsible entities have varying baselines, software vintages, and vendor support. Flexibility may be needed to prevent disruption of an entity's software update and patch management processes. SDT has added guidance in the technical guidelines section to support responsible entities in adding this objective to their configuration change management processes.	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
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	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
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	

Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 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	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE notes that the proposed standard is not responsive to the FERC directive. FERC Order No. 829 P. 59 specifically 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 Note in Part 1.6, however, states: "Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual *terms and conditions of a procurement contract*; and (2) vendor performance and adherence to a contract." Texas RE agrees that it is unreasonable to hold a registered entity accountable for a vendor's adherence to (or lack of adherence to) a contract. Texas RE agrees as the SDT claims obtaining specific controls in the negotiated contract may not be feasible at all times but Texas RE believes this is *best practice*. In fact, in most cases contracts for these types of systems typically include security provisions and set similar expectations as described in the	

standard. The proposed standards would prohibit the compliance monitor from verifying the registered entity implemented part 1.6. Moreover, this verification is to ensure that the registered entities' plans are consistent with the contract's expectations and obligations of the parties. Admittedly, there will be circumstances in which a contracts may not be consistent or silent as it pertains to the responsible entity's security management plans (e.g. existing contacts or contracts in which the responsible entity was unable to negotiate the appropriate terms into the contract.) In those circumstances, other evidence should be provided demonstrating that the responsible entity has processes to ensure the vendor is expected/obligated to act consistent with the responsible entity's cyber security risk management plans as it relates to the vendor's products or services. Therefore, the contracts should remain in scope as to demonstrate the mapping of expectations from the plan to the contract as far as vendor interactions for those specific items included in the standard and to advance best practices leading to a more reliable BES. Texas RE also recommends the SDT remove or provide clarity on the verbiage that reads, "*and when the method to do so is available to the Responsible Entity from the software source*". A potential scenario exists now where vendors will attest that identity and integrity methods are not available therefore Part 1.6 is not applicable. Texas RE notes that the words "integrity" and "authenticity" are used in the Guidelines and Technical Basis however Part 1.6 uses the words "identity" and "integrity". Are these intended to be the same?

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Part 1.6 applies to baseline changes after the effective date of the standard, regardless of whether the responsible entity has a contract with a vendor. The SDT believes the measures describe the acceptable evidence that should be used to assess responsible entity adherence to the software verification requirements.

SDT believes the phrase 'when a method to do so is available' provides responsible entities with necessary flexibility to perform configuration management obligations. Responsible entities have varying baselines, software vintages, and vendor support. Flexibility

may be needed to prevent disruption of an entity's software update and patch management processes, including obligations under CIP-007. The SDT revised the guidelines section to remove terms that are not consistent with Part 1.6
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power

Answer	
Document Name	

Comment
MEAG supports the answers and comments of Salt River Project.

Likes 0	
Dislikes 0	

Response

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT's removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments of the IRC.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies Comments - NERC Cyber Supply Chain Risk Management 2016-03.docx
Comment	
Malware inserted into the U.S. electric grid in year 2014 and into the electric grid and other assets in the Ukraine in December 2015 and December 2016 target nominally "low impact" assets producing high impact consequences. See integrated comments that address in part the need to upgrade protections for so-called "low impact" facilities. (Comment at end of document)	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for “industrial control system hardware, software, and services associated with bulk electric system operations”(P. 43). High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that	

reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities.	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
While the IRC members do not have Low Impact Bes Cyber Systems we have multiple interfaces with our Market Participants that do have Low Impact BES Cyber Systems. This, in turn represents, risk to our BES Cyber Systems. As such we recommend that CIP-013-1 apply to Low Impact BES Cyber Systems to reduce the supply chain risk not only to the Low Impact BES Cyber Systems but to the IRC member organization's BES Cyber Systems. Note: **PJM does not support this comment**.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for "industrial control system hardware, software, and services associated with bulk electric system operations"(P. 43). High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities	

retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities.

IESO	
Answer	
Document Name	

Comment
As the IESO does not have any low impact BES Cyber Systems we abstain from answering Yes or No to this question. However, we suggest the rationale for not including Low Impact Bes Cyber Systems is not clear. We also suggest that small to medium sized Responsible Entities have the most to gain from CIP-013 as they have the fewest resources to mitigate risks from the supply chain. While the IIESO does not have Low Impact Bes Cyber Systems we have multiple interfaces with our Market Participants that do have Low Impact BES Cyber Systems. This, in turn represents, risk to our BES Cyber Systems. As such we recommend that CIP-013-1 apply to Low Impact BES Cyber Systems to reduce the supply chain risk not only to the Low Impact BES Cyber Systems but to the IRC member organization’s BES Cyber Systems.

Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for "industrial control system hardware, software, and services associated with bulk electric system operations"(P. 43). High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

While the initial direction of CIP-013-1 is good and provides protection for High BCS and Medium BCS, similar Cyber Assets associated with Low impact BES Cyber Systems may represent vectors for attack to High BCS or Medium BCS if left unprotected. WECC understands the reluctance of industry to incorporate Low impact BCS and their component BCA and other Cyber Assets under the CIP-013-1 purview and supports remanding SCRM issues associated with Low impact BCS to the CIP-003 Standard Drafting Team for integration into R1.2 and R2 of that Standard to ensure SCRM is integrated into those BCS at a level commensurate with the risk posed to the reliability of the BES.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The SDT does not believe development of requirements for low impact BES Cyber Systems, under either the supply chain or the CIP Modifications project, provides necessary reliability benefit commensurate with costs.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Teresa Cantwell - Lower Colorado River Authority - 1	

Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Oxy agrees with the removal of low impact BCS from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. Oxy believes that for entities that have a mixture of high, medium and low impact assets, the low impact assets would inherently benefit from the requirements applicable to high and medium impact assets as a matter of normal business practice, as the high water mark will be applied when purchasing equipment and services. This will account for a large portion of low impact BES Cyber Systems. Oxy believes it is appropriate to address the supply chain requirements using this risk-based approach. Low impact BES Cyber Systems are categorized as low impact because they inherently pose a low risk to negatively impact the Bulk Electric System. Resources should focus on those systems that have the potential for significant adverse impact on the BES. Additionally, vendors will not differentiate their product as low, medium or high impact, so as vendors address the requirements of high and medium impact entities, low impact entities will acquire the same products and services as medium and high impact entities. If low impact BES Cyber Systems were included in CIP-013-1, the costs associated with compliance would far outweigh the risk posed to the BES, in both manpower and additional equipment and services.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
GTC supports NRECA comments: NRECA appreciates the SDT's efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
None	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Yes. Industry supply chain management advances that would impact low impact BES Cyber Systems would be addressed by vendors through the requirements for high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Timothy Reyher - Eversource Energy - 5	
Answer	Yes
Document Name	
Comment	
None	
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 agrees with the removal of low-impact BES Cyber Systems from the applicability of CIP-013-1. Low-impact BES Cyber Systems have been subject to a risk assessment and classified low-impact since they pose a minimal threat to the BES. Also, a Responsible Entity is not required to have an inventory list of its low-impact BES Cyber Systems. If this standard were to apply to low-impact BES Cyber Systems, this would likely create a situation wherein an inventory list is necessary. This would be a significant effort, which would not likely bolster the reliability of the grid, based on the limited impact lows present to the system.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
GRE appreciates the SDT's efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	

Comment	
Luminant believes it is appropriate to address the supply chain requirements using a risk-based approach. 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. In addition, there are many types of low impact Cyber Systems. If a decision was made to put them back into the standard, there would need to be extensive work on evaluating each of these types of systems in order to determine whether there is adequate benefit to reliability to offset the cost and burden of imposing supply chain requirements for these systems.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes

Document Name	
Comment	
IPC agrees that the applicability to Lows should be removed.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC supports NRECA's Comments of: NRECA appreciates the SDT’s efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

USI agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agree that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829.	
Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	
Response. Thank you for your comments.	
Don Schmit - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
NPPD supports the position of the MRO NSRF.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA appreciates the SDT's efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the removal of low impact BCS from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. SRP believes that for entities that have a mixture of high, medium and low assets, the low assets would inherently benefit from the additional requirements of medium and low requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have low assets only, there would not be additional requirements based on CIP-002 risk based approach. SRP believes that including lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items. Also, controls inherent to CIP-013 and previous CIP Standards that reduce the risk associated with lows.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
No comments	
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	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See Attached Comments.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro believes that focussing on Medium and High Impact BCS instead of Low Impact is a good place to start. If insufficient risk mitigation is found to be provided here, it can always be expanded later. However, BC Hydro does not believe CIP-013-1 itself is necessary given what entities will already be doing under the other CIP v5 standards	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE agrees with removing low-impact BCS from CIP-013-1 and agrees the current standard, as written, appropriately addresses the Commission's concerns as specified in Order No. 829. AE believes, for entities with a mixture of High, Medium and Low Impact BCS, the Low Impact B CA would inherently benefit from the additional requirements of Medium and Low requirements as a matter of normal business practices. Additionally, many contracts and master agreements are developed for all products and services purchased from a vendor. For entities with Low Impact BCS only, there would not be additional requirements based on the CIP-002 risk-based approach. AE believes including Low Impact BCS will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these devices. Also, controls inherent to CIP-013 and previous CIP Standards reduce the risk associated with Low Impact BCS.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
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 with the removal of low-impact BES Cyber Systems from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. SMUD believes that for entities that have a mixture of High, Medium and Low assets, the Low assets would inherently benefit from the additional requirements of Medium and Low requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have Low assets only, there would not be additional requirements based on CIP-002 risk based approach.

SMUD believes that including Lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items. Also, controls inherent to CIP-013 and previous CIP Standards that reduce the risk associated with Lows.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Tyson Archie - Platte River Power Authority - 5

Answer	Yes
Document Name	

Comment

PRPA agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. PRPA believes that for entities that have a mixture of High, Medium and Low assets, the Low assets would inherently benefit from the additional requirements of Medium and Low requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have Low assets only, there would not be additional requirements based on CIP-002 risk based approach.

PRPA believes that including Lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items. Also, controls inherent to CIP-013 and previous CIP Standards that reduce the risk associated with Lows.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
Santee Cooper agrees with the removal of low-impact BES Cyber Systems from CIP-013-1. Including low-impact BES Cyber Systems will require substantial resources by a Responsible Entity it identify and maintain an inventory list of items.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes

Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	

Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
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	

Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 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	
Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 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	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
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	Yes
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	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
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	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	

Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
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	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC – 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	

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	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE's opinion is that low impact BES Cyber Systems should be included in CIP-013-1 because industrial control systems monitor and operate BES Cyber Assets located at transmission substations, wind farms, and generation facilities. Texas RE noticed that Question 4 uses the words "hardware, computing and networking services", which are not found in CIP-013-1. Should they be used in CIP-013-1 instead of "equipment, products, and services"?	
Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for "industrial control system hardware, software, and services associated with bulk electric system operations"(P. 43). High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities. The SDT used wording in CIP-013-1 that is consistent with other CIP standards. The SDT did not use the wording from Order No. 829 because it could be potentially unclear to responsible entities.
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance

Answer	
Document Name	
Comment	

No comment	
Likes 0	
Dislikes 0	
Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	
Document Name	
Comment	
PJM chooses to abstain from this question as we have no low impact assets.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.	
Gregory Campoli - New York Independent System Operator - 2	
Answer	No
Document Name	
Comment	
Request a 24 month implementation due to budget cycles and technical controls for other CIP Standards.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Disagree with the Implementation Plan. Standard should have language stating whether or not software installed prior to enforcement must have identify/verification completed.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. CIP-010-3 R1 Part 1.6 applies to changes to baseline. Software verification of existing baseline is not in scope.	
Timothy Reyher - Eversource Energy - 5	
Answer	No
Document Name	
Comment	
Recommend changing this General Consideration from Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1. To Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note Implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request a 24 months implementation due to budget cycles and technical controls for other CIP Standards	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT revised the General Consideration section to incorporate the suggested wording, and included provisions for unplanned changes consistent with other CIP standards.	

The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
Recommend changing this General Consideration from Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1. To Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note Implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request a 24 months implementation due to budget cycles and technical controls for other CIP Standards	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response. Thank you for your comment.	

The SDT revised the General Consideration section to incorporate the suggested wording, and included provisions for unplanned changes consistent with other CIP standards. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
Performance requirements are too vague to be auditable. See related comments. (Comment at end of document)	
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 generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. SMUD feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers. SMUD is indicating a "no" response as the implementation plan does not include a pilot. The implementation of TCA CIP 010 R4 was difficult as entities did not have a model implementation to learn practical applications of the standard in operations. Other standards that had a pilot allowed entities to learn practical implementation decisions that would save money and time. Please note, SMUD is willing to participate as a pilot participant.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk. The purpose of the Implementation Plan is to propose the effective dates of the Reliability Standards. A pilot program could support entity implementation and would not impact the proposed effective dates. SDT has shared the recommendation for a pilot with NERC and ERO staff for consideration as plans are developed to support industry implementation.	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

It is uncertain when purchasing activities become subject to CIP-013-1. The proposed Implementation Plan states: "Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1."

Reclamation recommends that the "General Considerations" guidance contained in the Implementation Plan pertaining to purchasing activities be included in the proposed standard.

If the "General Considerations" guidance on purchasing activities becomes part of the proposed standard, Reclamation further recommends:

- A contract becomes within scope when the entity commences its formal contract process such as when a request for proposal or solicitation is issued.
- Any direct purchase and/or any repurposed equipment is within scope prior to connecting to the Bulk Electric System as a cyber asset.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT has revised the Implementation Plan to clarify when an entity's procurement actions become subject to CIP-013-1. The general consideration section now reads:

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment	
CIP-013 R2 and/or the Implementation Plan should contain “trigger” language for R2 that clarifies an entity must implement its R1 risk management plan(s) for new procurement contracts signed on or after the Effective Date of CIP-013. Entities with no new procurement contracts or no new in-progress procurements on the Effective Date should not be expected to be able to demonstrate compliance with R2 at that time.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. SDT has revised the Implementation Plan to clarify when an entity must implement its plans. The general consideration section now reads:

> *In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity’s plan) that begin on or after the effective date of CIP-013-1.*

The SDT agrees that entities should not be expected to demonstrate compliance with Requirement R2 if the entity has not initiated procurement processes when the requirement is effective.

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request a 24-month implementation due to budget cycles and technical controls for other CIP Standards	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Request a 24 months implementation due to budget cycles and technical controls for other CIP Standards	

Recommend changing this General Consideration from Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1. To Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note Implementation Plan does not handle unplanned changes such as IROLs or registration, etc.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT revised the General Consideration section to incorporate the suggested wording, and included provisions for unplanned changes consistent with other CIP standards. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	

FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
GRE and the NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the "Planned or Unplanned Changes Resulting in a Higher Categorization" section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan. Additionally, the absence of the "Applicable Facilities" section or other language that clearly indicates these standards/requirements do not apply to "low" entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards, and to clearly indicate the standards to not apply to entities that do not have any medium or high impact BES Cyber Systems.	

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Yes. Moving the implementation date from 12 to 18 months is consistent with the CIP v5 implementation timeline for implementations. Would low impact BES Cyber Assets that might be in scope in the future have similar implementation timeline or longer?	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT is not considering requirements or implementation periods for low impact BES Cyber Systems.	
Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
AECI supports NRECA's comments provided below: NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the “Planned or Unplanned Changes Resulting in a Higher Categorization” section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan. Additionally, the absence of the “Applicable Facilities” section or other language that clearly indicates these standards/requirements do not apply to “low” entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards, and to clearly indicate the standards to not apply to entities that do not have any medium or high impact BES Cyber Systems.	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
GTC supports NRECA comments: NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the "Planned or Unplanned Changes Resulting in a Higher Categorization" section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan. Additionally, the absence of the "Applicable Facilities" section or other language that clearly indicates these standards/requirements do not apply to "low" entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards, and to clearly indicate the standards to not apply to entities that do not have any medium or high impact BES Cyber Systems.	

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern recommends that the SDT consider addressing previous issues with the Implementation Plan versions between CIP V5, V6, V7, etc., where Implementation Plans were “chained” together and there was not an Implementation Plan that contained all the necessary requirements in a single source. Southern strongly recommends producing a consolidated Implementation Plan.

Southern recommends that NERC and the SDT(s) consider addressing issues with the Implementation Plan versions between CIP V5, V6, V7, and Supply Chain, as Implementation Plans are “chained” together and there is no one Implementation Plan that contains all the necessary requirements in a single source. Implementation Plans for the CIP standards cover several important areas:

Implementation schedules of new or modified CIP standard requirements.

Implementation schedules for newly identified cyber assets brought into scope with current requirements based on planned or unplanned changes in the BES assets, or those from newly registered NERC entities. (previously known as IPFNICANRE – Implementation Plan for Newly Identified Cyber Assets or Newly Registered Entities)

Implementation schedules for BES Cyber Systems already in scope that change impact levels due to planned or unplanned changes in the BES.

As an example, the last page of the Implementation Plan for CIP-003-7 states that CIP-003-6 is retired upon approval of CIP-003-7, yet it chains to the CIP-003-6 Implementation Plan to tell entities how to handle cyber systems that change impact categorization. The CIP-003-6 implementation plan simply says it replaces *parts* of the V5 implementation plan for the modified standards in that revision. Only the V5 plan addresses the 2nd bullet point above. Responsible Entities are left to unravel three different plans with supply chain adding yet another to get one picture of what is due when and knowing how to handle BES changes that affect cyber system identification and impact categorization.

As we go forward, we need a better solution. Parts of an implementation plan, such as bullets 2 and 3 above, need to live on indefinitely. Other parts, such as the schedule of new or modified requirements, need to live until those dates have passed. Chaining all

of this together through numerous documents as the CIP standards continue to evolve and grow to cover new areas is not a sustainable solution that promotes clarity in knowing the compliance obligation in a changing environment.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees that Implementation Plans should avoid or, at a minimum provide clear details of, any overlap with pending effective dates of pending Reliability Standards requirements so that entities have clarity on the impact of implementation on their compliance obligations. The proposed Project 2016-03 Implementation Plan is not tied to requirements that have future effective dates, thereby avoiding some of the expressed concerns. Furthermore, the Implementation Plan has been revised to include provisions for unplanned changes so that it is not reliant on these provisions from Implementation Plans associated with other standards.	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Disagree with the Implementation Plan. Standard should have language stating whether or not software installed prior to enforcement must have identify/verification completed.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. CIP-010-3 R1 Part 1.6 applies to changes to baseline. Software verification of existing baseline is not in scope.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	

Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes

Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	

Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT joins the comments of the IRC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	

Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
As mentioned above, WECC supports the CIP-013-1 implementation plan, including the expectation for the initial performance of the R3 review and approval on or before the effective date.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes

Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
We agree with APPA's submitted comments, including: Suggesting a change in wording to say that the Supply Chain Risk Management Plan must be used on or after the implementation date rather than saying that contracts on or after that date are within scope of CIP-013. Clarification should be made about if/when existing contracts or agreements come into scope.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the General Considerations section in the Implementation Plan as follows: *In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of*	

cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	
PRPA generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. PRPA feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE generally agrees with an 18-month implementation plan but, would prefer 24-months. AE feels a 24-month timeframe is more appropriate and gives entities additional time to align budgets and develop processes with vendors and suppliers. As a municipal utility, AE's procurement process is quite long.	

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk. The SDT also believes the flexibility provided in the requirements supports the various procurement processes that may be used by responsible entities.

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx

Comment

See attached comments

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT revised the General Consideration section to incorporate the suggested wording, and included provisions for unplanned changes consistent with other CIP standards.

The SDT has revised the General Considerations section in the Implementation Plan as follows:

> *In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.*

Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	

Recommend changing this General Consideration from

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To

Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date of the CIP-013-1. Make corresponding change to the CIP-013 R2 note.

And

CIP-005-6 and CIP-010-3 must be implemented 18 months after the implementation date of the CIP-013-1

Implementation Plan does not handle unplanned changes such as IROLs or registration, etc.

Request a 24 month implementation of CIP-013-1 due to budget cycles and technical controls for other CIP Standards

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT revised the General Consideration section to incorporate the suggested wording, and included provisions in the Implementation Plan for unplanned changes consistent with other CIP standards.

The SDT does not believe it is necessary to delay implementing CIP-005-6 and CIP-010-3 until after CIP-013-1. Procurement actions taken according to the entity's Supply Chain Cyber Security Risk Management Plan can support the new requirements in CIP-005-6 and CIP-010-3, however the new CIP-005-6 and CIP-010-3 requirements are written so that they are not dependent on these procurement actions.	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. SRP feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
While in overall agreement with the updated Implementation Plan, ACEC does have the following concern:	

The second paragraph in the section "General Considerations" states "Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1." Based upon the above wording it could be understood that Master Supply Agreements (MSAs) would need to be changed in the first RFP after implementation of the new standard. The paragraph should state specifically that this is not required, and that the plan can allow MSAs to exist as is until it is time to review in the normal procurement process.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the General Considerations section in the Implementation Plan as follows: *In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.*	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the "Planned or Unplanned Changes Resulting in a Higher Categorization" section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan. Additionally, the absence of the "Applicable Facilities" section or other language that clearly indicates these standards/requirements do not apply to "low" entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.	

Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards, and to clearly indicate the standards to not apply to entities that do not have any medium or high impact BES Cyber Systems.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Thank you for your statement under Initial Performance of Periodic Requirements, that the supply chain security risk management plans need to be approved on or before the effective date of CIP-013-1.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
Don Schmit - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Comments: NPPD supports the position of the MRO NSRF. NPPD believes a 24-month implementation should be used due to budgeting and tthe technical implementation requirements for the other CIP Standards.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Recommend changing this General Consideration from:	

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To:

Supply Chain Risk Management plan must be used by appropriate procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note.

Further, USI requests clarification on if/when existing contracts, master contracts, or long-term maintenance agreements that re-opened for renegotiation or put in use, come into the scope of CIP-013.

The implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request that the Implementation Plan be modified to handle entities that meet the applicability after the effective date of the standard.

USI believes a 24-month implementation should be used due to budget cycles and technical controls for other CIP Standards.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response. Thank you for your comment. The SDT has revised the General Considerations section in the Implementation Plan as follows:

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.

The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards.

The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.

Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

GSOC supports NRECA's Comments of:

NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the "Planned or Unplanned Changes Resulting in a Higher Categorization" section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan.

Additionally, the absence of the "Applicable Facilities" section or other language that clearly indicates these standards/requirements do not apply to "low" entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards, and to clearly indicate the standards to not apply to entities that do not have any medium or high impact BES Cyber Systems.

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

NRG recommends changing this General Consideration from:

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To

Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Please consider making the corresponding change to the CIP-013 R2 note

The Implementation Plan does not appear to address unplanned changes such as IROLs or registration, etc.

NRG requests consideration of a 24 month implementation due to budget cycles and technical controls for other CIP Standards

Likes 0	
Dislikes 0	

Response, Thank you for your comment. The SDT has revised the General Considerations section in the Implementation Plan as follows:

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.

The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards.

The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
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	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
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	
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	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 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	

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
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	

Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 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	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 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	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
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	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
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	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE requests that the SDT provide its rationale for extending the effective date from 12 to 18 months. For example, it is unclear whether the SDT believes more certainty is required regarding the necessary technical deployments for compliance with the Standard as some commenters suggested to justify the extended implementation period.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees with commenters that the proposed requirements can be impacted by budget cycles, which can extend beyond 12-months. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	

Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment
ERCOT joins the comments of the IRC.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment
Duke Energy suggests the drafting team consider implementing a staggered approach to the VSL(s) specifically to CIP-013-1 R2. As written, an entity could implement all aspects but one sub-part of the risk management plan, and the violation would have a VSL of Severe. We recommend the drafting team consider a more equitable approach and stagger the VSL(s) similar to the approach used in R1 of CIP-003-6.

Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT has revised the VSL for CIP-013-1 Requirement R2 to specify four levels of possible non-compliance.	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
We do not agree with the VRF Justification for CIP-013-1 R1, FERC VRF G5 with the new redline. Agree with the words that were redline out.	

CIP-010 – VSL does not cover the failure to implement the process and therefore does not include all of the combinations. Consequently, we request that there be lower severity levels when a single aspect of the requirements is missing. Request that that the term “elements” be included in CIP-013 R1.2 (as shown in comments for question 1) to clearly align with the VSLs for this requirement.	
Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	
Response. Thank you for your comment. The SDT agrees with the suggested change to the VRF justification for CIP-013-1 Requirement R1. For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See attached comments	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2. For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1. The SDT agrees that another level can be specified for CIP-005-6 and has revised the VSL accordingly.	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
The VSL for R2 only provides for a Severe VLS. It is unclear what is meant by "did not implement". If your plan has 5 areas within it and 4 of the 5 were fully implemented, has the plan been implemented? I contend yes however not fully implemented. The VSL were created to identify how far of the complaince mark an entitiy fell. This VLS completly fails to perform this action. While at the same time the VSL for R3 utilizes arbitrary calendar months for clear VLS seperation between lower and severe. Both of these VLS provide little benefit to industry in assessing the real impact to the BES based on an entity missing the complaince mark.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the VSL for CIP-013-1 Requirement R2 to specify four levels of possible non-compliance.	

Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
We support APPA's comments that the original wording is better than the new redline of the VRF justification.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees with the suggested change to the VRF justification for CIP-013-1 Requirement R1.	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
While an important topic, at this time AEP does not agree that risks associated with violations of these draft standards is a “Medium” risk to the BES. AEP recommends the Violation Risk Factor for each of the requirements CIP-013-1 R 1-3 be considered “Lower.”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT developed the VRFs to conform to NERC and FERC guidelines as explained in the VRF/VSL Justification.	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD asks that that the term “elements” be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement. “***1.2.*** *One or more process(es) for its newly procured BES Cyber Systems that address the following elements, as applicable:”*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
: For CIP-013-1, R3, Dominion recommends the following alternate VSL values. • Low – No change • Moderate – 16-18 calendar days • High – greater than 18 calendar days	

• Severe – When a review has never been performed	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT established the levels to be consistent with approved CIP standards and does not see benefit to adopting alternate levels.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD asks that that the term "elements" be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement. "***1.2.*** *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:"*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has removed the term 'elements' from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD asks that that the term “elements” be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement. “***1.2.*** *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:”*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD asks that that the term “elements” be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement. “***1.2.*** *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:”*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	No
Document Name	

Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
No additional comments.	

Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
The IRC suggests the drafting team add more thresholds to the VSLs for R2 of CIP-013-1 and that it be aligned more closely with that of R1, rather than making it binary. The cyber security risk management plan will be fairly large and missing small portions of the plan should not immediately result in a Severe VSL.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the VSL for CIP-013-1 Requirement R2 to specify four levels of possible non-compliance.	
IESO	
Answer	Yes
Document Name	
Comment	

None	
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	
Answer	Yes
Document Name	
Comment	
None	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	

Dislikes 0	
Response	
Timothy Reyher - Eversource Energy - 5	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
There should be lower, moderate and high VSLs for R2, (not implementing portions of the requirement). PJM suggests using the language in the lower, moderate and high R1 VSLs as a starting point.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT has revised the VSL for CIP-013-1 Requirement R2 to specify four levels of possible non-compliance.	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Yes for CIP-005-6 and CIP-010-3 only	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	

Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

No Comments	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
YES for CIP-005-6 and CIP-010-3 only	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the VRFs and VSLs for CIP-010 and CIP-013. SRP believes that the VRFs and VSLs for CIP-005 should be updated to reflect the same approach that was taken in CIP-010. The VSL for CIP-005 results in a severe penalty if the entity did not have a method to	

determine and did not have a method to disable. SRP would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable. SRP requests that the term “elements” be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees that another level can be specified for CIP-005-6 and has revised the VSL accordingly. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE agrees with the VRFs and VSLs for CIP-010 and CIP-013. AE believes the VRFs and VSLs for CIP-005 should be updated to reflect the same approach taken in CIP-010. The VSL for CIP-005 results in a severe penalty if an entity does not have a method to determine and does not have a method to disable. AE would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable. AE requests the term “elements” be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.	
Likes 0	
Dislikes 0	

Response Thank you for your comment. The SDT agrees that another level can be specified for CIP-005-6 and has revised the VSL accordingly. The SDT has removed the term 'elements' from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
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 with the VRFs and VSLs for CIP-010 and CIP-013. SMUD believes that the VRFs and VSLs for CIP-005 should be updated to reflect the same approach that was taken in CIP-010. The VSL for CIP-005 results in a severe penalty if the entity did not have a method to determine and did not have a method to disable. SMUD would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable. SMUD requests that the term "elements" be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT agrees that another level can be specified for CIP-005-6 and has revised the VSL accordingly. The SDT has removed the term 'elements' from the VSL for CIP-013-1 Requirement R1 Part 1.2.	

Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	
PRPA agrees with the VRFs and VSLs for CIP-010 and CIP-013. PRPA believes that the VRFs and VSLs for CIP-005 should be updated to reflect the same approach that was taken in CIP-010. The VSL for CIP-005 results in a severe penalty if the entity did not have a method to determine and did not have a method to disable. PRPA would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable. PRPA requests that the term “elements” be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT agrees that another level can be specified for CIP-005-6 and has revised the VSL accordingly. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	

No Comment.	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
WECC has no issues with the VSLs or VRFs from a CIP Auditor perspective.	
Likes 0	

Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Harris - Foundation for Resilient Societies - 8	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
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	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
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	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
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	Yes
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	

Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 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	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	

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	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
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	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	

Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	No
Document Name	
Comment	
The requirements aren't vetted enough to make a fair judgement.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Timothy Reyher - Eversource Energy - 5	
Answer	No
Document Name	
Comment	
Implementation Guidance for R3	

Neither main bullet meets compliance because both only deal with the review and not the approval. Recommend changing “Below are some examples of approaches to comply with this requirement:” to “Below is an example of an approach to comply with the review requirement required by:” Implementation Guidance for R3 – Recommend removing this language from the second main bullet, since it is beyond the Requirement “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. NERC Compliance Guidance Policy provides a means for any NERC registered entity to document examples of approaches and vet them through an approved organization for endorsement consideration by the ERO Enterprise.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	No
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No

Document Name	
Comment	
CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	

CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The existing guidance still provides no scope of cyber security risks that should be considered, and without context, many of the proposed actions have no guidelines or measurements for "success" or "failure" or acceptability; nor are there suggested acceptable mitigations if a criterion is not completely met, since there is no clear objective. Furthermore, there is no allowance made for a continuous process, where, as a result of products already being used in BES Cyber Systems and subjected to the existing CIP standards, cyber security risks	

associated with networks, products and vendors are evaluated on an on-going basis. Detailed changes and additions are outlined in a separate redline Draft Implementation Guidance document that has been forwarded to NERC and the SDT. A summary of the proposals is as follows:

1. Throughout the document, the term 'controls' should be changed to a term that more closely reflects the language in the proposed standard. Dominion recommends using 'terms and conditions'.
2. On page 2, dominion recommends clarifying that cyber security risks are limited to supply chain with the addition of 'supply chain' prior to each use of the term cyber security risks.
3. In addition to the clarifying language in item #2 above, Dominion recommends adding the following to more clearly define the term 'supply chain cyber security risk:

(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). The additional bullets could be sub-bullets under the appropriate of these four broad areas as examples rather than individual, isolated items.

4. Dominion recommends deleting the third paragraph on page 2. This paragraph appears to be creating new/different obligations. The language appears to create confusion and calls out Section 1.2.5 specifically for no apparent reason.

5. The language in blue boxes throughout the document should be retained and included in the text of the document.

6. It is unclear what the purpose of including certain language in a blue box is.

7. Section headings should be included with each of the examples. Also, the bulleted format makes it unclear if one, all, or a certain number of bulleted items need to be performed to achieve compliance.

8. Add the following example under R1.1:

Develop an approved vendor/products list. When planning a BCS, the RE should evaluate the following items:

-
  - Vendors
  - Products
  - Network Architecture
  - Network Components.

The RE should document (which may be limited to the baseline and cyber vulnerability assessment (CVA) required for a new product) any risks (i.e. 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) identified and how the risks are mitigated for any "item" that deviates from those vendors, products, network architecture, and network components already being used within the RE's BCS infrastructures, which are required to comply with existing CIP standards.

9. The second bullet in Section 1.2.2 should be removed. It is already addressed under Section 1.2.1.

10. In Section 1.2.3, the end of the first bullet could state be clarified as follows:

Delete 'within a negotiated period of time of such determination' and replace with "to allow the RE to remove access within 24 hours of the determination, consistent with existing CIP standards"

Replace 'breaches' with 'vulnerabilities' for clarity and consistency'.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. Per NERC's Compliance Guidance Policy, various organizations are qualified to vet proposed Implementation Guidance prior to requesting ERO Enterprise endorsement.	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.	

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
The Implementation Guidance only identifies items that could be evaluated in developintg a Supply Chain Cyber Security program, but does not provide an example or guidance on how to implement the program. Without this guidance, it is impossible to understand how to comply with CIP-013-1 in a cost-effective and compliant manner.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the Implementation Guidance describes examples of how to implement the requirements.	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
We agree with APPA's submitted comments concerning "vendor" not being a NERC-defined term and that the Implementation Guidance for R3 does not adequately explain compliance needs.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro does not agree with the examples as compliance will be challenging. It would require us to have sufficient authority over the vendor (which will not be the case in most situations). There is also no way to ensure that a vendor is being completely transparent regarding cyber vulnerabilities in their product. Such disclosure could have other impacts on their business with other clients. This would be a dis-incentive for disclosure. BC Hydro does not believes CIP-013 is necessary and cyber control is already achieved with the rest of the CIP v5 standard requirements around change control, testing and ongoing systems monitoring.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the examples provided in the ERO-Enterprise endorsed Compliance Guidance can be implemented by responsible entities using their procurement processes. The requirements in CIP-013-1 do not require responsible entities to impose obligations on vendors. The requirements address the reliability objectives contained in the project Standards Authorization Request.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See attached comments.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.

The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. NERC Compliance Guidance Policy provides a means for any NERC registered entity to document examples of approaches and vet them through an approved organization for endorsement consideration by the ERO Enterprise.

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

It is uncertain when purchasing activities become subject to CIP-013-1. The proposed Implementation Plan states: “Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.”

Reclamation recommends that the “General Considerations” guidance contained in the Implementation Plan pertaining to purchasing activities be included in the proposed standard.

If the "General Considerations" guidance on purchasing activities becomes part of the proposed standard, Reclamation further recommends: • A contract becomes within scope when the entity commences its formal contract process such as when a request for proposal or solicitation is issued. • Any direct purchase and/or any repurposed equipment is within scope prior to connecting to the Bulk Electric System as a cyber asset.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Response is provided in preceding section.	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
There is inconsistency between the Implementation Guidance and CIP-010, R1. The requirement states "For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5". The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches." The requirement wording suggests it applies for any change but the Guidance suggests that for some changes, such as patches, it would not apply. Oncor believes that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore, it is believed that the best solution is to modify the Guidance.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT has not developed Implementation Guidance for CIP-010-3. The CIP-010-3 Measure and the Guidelines and Technical Basis section have been revised to address the stated concern with automated patch management.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005. USI believes the SDT should provide guidance regarding the use of the term “vendor.” If “Vendor” is not defined by NERC, the Guidance should recommend that Entities include their definition of “vendor” in their plan(s). **Implementation Guidance for R3** Neither main bullet meets compliance because both only deal with the review and not the approval. Therefore, USI recommends changing: ”Below are some examples of approaches to comply with this requirement: “ to “Below is an example of an approach to comply with the review requirement required by: “ In addition, we recommend removing this language from the second main bullet, since it is beyond the Requirement: “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.” Also, there should be corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.	
Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response. Thank you for your comment.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs.

The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address the concerns. NERC Compliance Guidance Policy provides a means for any NERC registered entity to document examples of approaches and vet them through an approved organization for endorsement consideration by the ERO Enterprise.

CIP-005-6 includes Rationale. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	

- The language within the Implementation Guidance contradicts the language within CIP-013. (i.e. System-based approach). The Implementation Guidance is not auditable, however, the Standard and Requirements are. EDPR NA suggests that the Implementation Guidance is eliminated and further support are provided within the Measures for a Registered Entity and auditor's reference.
- There are numerous items in which vendors will not provide information on unless an entity is willing pay significant increases (risks, training, methodologies, threats, etc.)

• EDPR NA also suggests that NERC utilize a pilot program to test these requirements prior to enforcing the implementation of CIP-013 to all Registered Entities. • Please provide more support with respect to the expectations and possible evidence for Requirement 2.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. Furthermore, ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) staffs give deference to the examples in endorsed guidance when conducting compliance monitoring activities. The SDT believes an entity can use a system-based approach in its Supply Chain Cyber Security Risk Management plan(s) as described in the Implementation Guidance to comply with Requirement R1. The examples provided in the ERO-Enterprise endorsed Compliance Guidance can be implemented by responsible entities using their procurement processes. The requirements in CIP-013-1 do not require responsible entities to impose obligations on vendors. CIP-013-1 does not obligate entities to obtain specific contract provisions, preserving entity flexibility to make cost decisions. The SDT agrees that a pilot program could support entity implementation and would not impact the proposed effective dates. SDT has shared the recommendation for a pilot with NERC and ERO staff for consideration as plans are developed to support industry implementation. The examples of approaches described in the section titled 'Implementation Guidance For Requirement R1', when used in planning and procurement as specified in the entity's plan, provide an example of a compliance approach to meeting Requirement R2.	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No

Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	

There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1.

The requirement states, in relevant part, “For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5.”

The Guidelines and Technical Basis section heading “Software and Authenticity,” paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.” The wording of the CIP-10-3 R1.6 Guidelines and Technical Basis section seems to imply that every time a patch/software is downloaded it does not have to be checked. Based on how the standard is written, the software source and the software must be verified each time something is downloaded. Even if that software was previously downloaded, the source must be validated and so must the software before application.

Furthermore, the requirement wording suggests it applies for any change but the Guidelines suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the Guidelines are not, the Guidelines become superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. SPP recommends that the SDT review the Guidelines and the draft standard for consistency and resolution. In addition, SPP recommends that because automated patch deployment solutions should be able to verify the identity and integrity of the patch, the SDT consider allowing for this method of verification in the Measures or Guidelines. SPP notes that there is no corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-010-3 Measure and the Guidelines and Technical Basis section have been revised to address the stated concern with automated patch management. CIP-005-6 includes Rationale. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG has concerns that the Implementation Guidance for R3 (main bullet) may not meet compliance because both only deal with the review and not the approval. NRG recommends that the NERC SDT consider changing "Below are some examples of approaches to comply with this requirement:" to "Below is an example of an approach to comply with the review requirement required by:"	

NRG has concerns that the Implementation Guidance for R3 – (specifically): "Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed." Therefore, NRG recommends that the NERC SDT consider removing this language from the second main bullet, since it is beyond the Requirement. There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1. The requirement states, in relevant part, "For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5." The Guidelines and Technical Basis section heading "Software and Authenticity," paragraph three on page 39, states: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches." The wording of the CIP-10-3 R1.6 Guidelines and Technical Basis section seems to imply that every time a patch/software is downloaded it does not have to be checked. Based on how the standard is written, the software source and the software must be verified each time something is downloaded. Even if that software was previously downloaded, the source must be validated and so must the software before application. Furthermore, the requirement wording suggests it applies for any change but the Guidelines suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the Guidelines are not, the Guidelines become superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. NRG recommends that the SDT review the Guidelines and the draft standard for consistency and resolution. In addition, NRG recommends that because automated patch deployment solutions should be able to verify the identity and integrity of the patch, the SDT consider allowing for this method of verification in the Measures or Guidelines. NRG notes that there is no corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. The CIP-010-3 Measure and the Guidelines and Technical Basis section have been revised to address the stated concern with automated patch management. CIP-005-6 includes Rationale. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
ITC Holdings agrees with the below comment submitted by SPP: There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1. The requirement states, in relevant part, “For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5.” The Guidelines and Technical Basis section heading “Software and Authenticity,” paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.” The wording of the CIP-10-3 R1.6 Guidelines and Technical Basis section seems to imply that every time a patch/software is downloaded it does not have to be checked. Based on how the standard is written, the software source and the software must be verified each time	

something is downloaded. Even if that software was previously downloaded, the source must be validated and so must the software before application. Furthermore, the requirement wording suggests it applies for any change but the Guidelines suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the Guidelines are not, the Guidelines become superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. SPP recommends that the SDT review the Guidelines and the draft standard for consistency and resolution. In addition, SPP recommends that because automated patch deployment solutions should be able to verify the identity and integrity of the patch, the SDT consider allowing for this method of verification in the Measures or Guidelines. SPP notes that there is no corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-010-3 Measure and the Guidelines and Technical Basis section have been revised to address the stated concern with automated patch management. CIP-005-6 includes Rationale. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
As stated in the CIP-013 comments in question 1 above, the guidance needs to clarify what constitutes an incident (such as only actual breaches).	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Yes, and BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not "plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require the responsible entity's CIP Senior Manager to review and approve the controls adopted to meet the specific security objectives identified in the Reliability Standard at least every 15 months." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply	

only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
The understanding of the intent and purpose of CIP-013 is very dependent on the Implementation Guidance document. We are concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such we would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards	

development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
The Guidance for CIP-013-1 R3 should include the term 'approved' since an Entity wouldn't comply with the requirement with just a review.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	

Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Yes, the Compliance Guidance policy does provide industry with direction for implementation. However, those guidance details are not written in the requirements, measures or Reliability Standard Audit Worksheet (RSAW) and cannot be relied upon in preparation of an audit. ACES would suggest, at a minimum, that these guidelines be written in the Supply Chain Management RSAWs in the section 'Notes for an Auditor'. By placing this information in the RSAW, it gives industry additional reassurance that each region will audit Supply Chain Management consistently.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees and will provide this feedback to the RSAW Task Force.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Implementation Guidance for R3	

Neither main bullet meets compliance because both only deal with the review and not the approval. Recommend changing “Below are some examples of approaches to comply with this requirement:” to “Below is an example of an approach to comply with the review requirement required by:” Implementation Guidance for R3 – Recommend removing this language from the second main bullet, since it is beyond the Requirement “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns.	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	

Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes

Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment	
ERCOT joins the comments of the IRC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Implementation Guidance for R3	

Neither main bullet meets compliance because both only deal with the review and not the approval. Recommend changing “Below are some examples of approaches to comply with this requirement:” to “Below is an example of an approach to comply with the review requirement required by:” Implementation Guidance for R3 – Recommend removing this language from the second main bullet, since it is beyond the Requirement “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns.	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
For consistency and clarity between sub-requirement 1.2.2. and the CIP-013-1 Implementation Guidance, we suggest that “cyber security incident(s)” be removed from the examples for 1.2.2. This verbiage should be replaced with either “vendor-identified incidents” or “security event(s)” as referenced in the examples for 1.2.1.	
Likes 0	

Dislikes 0	
Response Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The responsible entity has flexibility to use its preferred wording in its cyber security supply chain risk management plan.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
The guidance relative to R1.2.2 and R1.2.6 partially address WECC's concerns as stated in Bullet 2 above. In general, the example approaches provide good guidance to industry on ERO expectations for compliance with the various Requirements and Parts. No other issues noted.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
The intent and purpose of CIP-013 is very dependent upon the Implementation Guidance document. We appreciate the hard work of the SDT to provide this document to industry and it has valuable information. Additionally, there is no guarantee this document will be approved by NERC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	

Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	

PRPA generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. PRPA is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, PRPA would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.

R3: PRPA requests that the following language be removed from the second main bullet, since it is out of scope for this Requirement. "Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed."

Request that there be corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-010-3 R1.6.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not

duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. The SDT has included Rationale for CIP-005-6 Requirement R2 Parts 2.4 and 2.5, and both Rationale and Guidelines and Technical Basis for CIP-010-3 R1.6. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
In the guidance for Requirement R1, Part 1.2.5, CenterPoint Energy believes including all third-party hardware, software, firmware, and services goes beyond the scope of the requirement. Most systems consist of components or services from numerous third-party companies. The vendor of such systems may not have direct contact with third-party companies. The level of third-party components or services that could be expected to be included may be quite extensive and therefore make it impractical for the vendor to commit to such issues in contract provisions.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT believes the examples in the Implementation Guidance for Part 1.2.5 show a way for a responsible entity to seek information through its procurement processes that may be helpful in addressing a valid security concern associated with vendor software. Responsible entities may use other approaches to meeting the obligation of Part 1.2.5.	
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 generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. SMUD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, SMUD would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard. R3: SMUD requests that the following language be removed from the second main bullet, since it is out of scope for this Requirement. “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.” SMUD also requests that there be corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-010-3 R1.6.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. The SDT has included Rationale for CIP-005-6 Requirement R2 Parts 2.4 and 2.5, and both Rationale and Guidelines and Technical Basis for CIP-010-3 R1.6. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. AE has concerns about the possibilities NERC and the Regions: (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, AE would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard.	

R3: AE requests the following language be removed from the second main bullet, because it is out-of-scope for this Requirement: "Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed." AE requests there be corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2, Parts 2.4 and 2.5 and CIP-010-3 R1.6.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. The SDT has included Rationale for CIP-005-6 Requirement R2 Parts 2.4 and 2.5, and both Rationale and Guidelines and Technical Basis for CIP-010-3 R1.6. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes

Document Name	
Comment	
Make sure the Compliance Guidance is in the scope of standards.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
As mentioned in previous comments, this document provides implementation guidance on CIP-013, but additional guidance on implementation of the CIP-010 and CIP-005 controls is requested, perhaps in the Supplemental Material sections. Particularly CIP-005 R2.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The CIP-010-3 Guidelines and Technical Basis section has been revised to provide additional guidance. CIP-005-6 includes guidance in the Rationale section for Requirement R2. The Rationale will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
SRP generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. SRP is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, SRP would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard. R3: SRP requests that the following language be removed from the second main bullet, since it is out of scope for this Requirement. "Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed." Request that there be corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-010-3 R1.6.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards	

development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. The SDT has included Rationale for CIP-005-6 Requirement R2 Parts 2.4 and 2.5, and both Rationale and Guidelines and Technical Basis for CIP-010-3 R1.6. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Yes, and BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not "plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require the responsible entity's CIP Senior Manager to review and approve the controls adopted to meet the specific security objectives identified in the Reliability Standard at least every 15 months." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. Requirement R3 addresses the Order No. 829 directive for requiring CIP Senior Manager review and approval of the plan. (P. 46). The SDT believes it is appropriate to allow entities to have flexibility in determining whether the CIP Senior Manager or delegate should review and approve the plan. CIP-003-6 provides for policy review by CIP Senior Manager only	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
While in overall agreement with the Implementation Guidance for CIP-013, ACEC does have the following concern: In the Implementation Guidance for R1 Section of the document, the subsections for implementation of Requirement R1 Parts 1.2.1, 1.2.2, 1.2.4 and 1.2.5 use the generic term “vendor(s)” in discussing these Software Authenticity and Integrity issues. To help in ensuring that these requirements are implemented in an effective manner, it is recommended that the SDT add a clarification item, noting that these requirements be addressed by the OEM providing the hardware and/or software, not a third-party such as an integrator.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the ERO-Enterprise endorsed Implementation Guidance provides appropriate guidance as written and does not limit the responsible entity’s flexibility to address relevant security topics with the OEM. However the SDT believes it may not be practical for responsible entities to address the security topics with the OEM because the responsible entity may not have a relationship with the OEM that will allow the responsible entity to address the topics through its procurement processes.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	

Comment	
N&ST has no disagreement with the example approaches contained in the Guidance but believes that while they may represent reasonable courses of action for large entities, they are likely to be far beyond the capabilities of small ones. N&ST believes an entity whose combined BES operations, OT support, and CIP compliance teams comprise fewer than 10 individuals would be hard-pressed to "form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es)." N&ST also believes, based on experience with CIP V1 – V5 cyber security training requirements, that large vendors with many BES customers will balk, sooner or later, at being asked to respond to a multitude of risk assessment requests, questionnaires, meetings, etc., each one different from the previous ones, and will instead incline towards providing a standardized set of information about their internal risk management programs and how they are applied to their products and services.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The examples in the Implementation Guidance describe some ways to be compliant with CIP-013-1. The SDT agrees that the examples may not be the most efficient or effective approaches for all responsible entities. The SDT believes including relevant cyber security topics in the procurement processes will provide reliability benefit even if some vendors do not provide all of the desired information or support requested terms.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment.	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon thanks the SDT for submitting the draft Implementation Guidance for CIP-013. Does the SDT also intend the develop draft Implementation Guidance for the revised/added sections of CIP-005 and CIP-010? If so, is there a timeline that can be shared with Industry participants?	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT is not developing Implementation Guidance for CIP-005 and CIP-010.	
Stephanie Little - Stephanie Little	
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	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 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	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

IESO	
Answer	Yes
Document Name	
Comment Note: the following comment is the same as identified for question 3.	
None	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 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	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
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	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
We consider the requirements to be burdensome, and impractical for many or most electric utilities without providing needed protection of the cyber supply chain. We would suggest at the outset adoptioon of a separate FERC rulemaking to detect, report, mitigate and remove malware from the bulk electric system.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
By placing those comments and guidance in the Implementation Guidance does not provide industry protection during an audit in defining ‘cost effective manner’. If it is important to communicate to industry that Supply Chain Management can be managed in a ‘cost	

effective manner', then that should be detailed in the standards. 'Cost effective manner' is an undefined term and will be different for each entity, budget and their resources. The focus should be modified to a 'risk reduction manner' or 'risk appropriate manner'.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	No
Document Name	
Comment	
There is not enough clarity in the proposed language to make that assessment.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

NRG is cognizant and appreciative of the flexibility provided in proposed CIP-013-1 and the draft Implementation Guidance but at this time cannot speak to whether the implementation of these requirements will be cost effective. Additional internal analysis is needed to inform NRG's evaluation as to the cost-effectiveness of the proposal.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
SPP is cognizant and appreciative of the flexibility provided in proposed CIP-013-1 and the draft Implementation Guidance but at this time cannot speak to whether the implementation of these requirements will be cost effective. Additional internal analysis is needed to inform SPP's evaluation as to the cost-effectiveness of the proposal.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	

By asking vendors to enforce these requirements, service costs will dramatically increase which will put a further strain on the electric industry.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Don Schmit - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
This new standard will put additional burden on entities. It is going to take considerable time to implement and negotiate new contracts. It is also up to the entity to provide adequate documentation to prove compliance but it will still be based on the auditor discretion if an entity has done enough. As with similar requirements in the nuclear industry we believe that contract pricing will increase due to the Standard requirements placed on the vendors via industry and may result in reduction of vendor options.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST believes the approaches to meeting CIP-013's reliability objectives described in the Implementation Guidance could easily consume scores, if not hundreds, of staff hours, with the potential to make "vendor risk assessment(s)" a significant cost component of any large-scale procurement. N&ST notes that although most of the documents referenced in the Guidance document are available for download at no charge, the Shared Assessment Program's Standardized Information Gathering (SIG) questionnaire, referenced in a footnote, must be purchased for $6,000. The Guidance document does point out that a Responsible Entities are free to pursue different approaches to CIP-013 implementation that "better fit their situation," but provides no examples of alternatives that might be worth considering. N&ST encourages NERC and the SDT to consider how utilities with very small staffs and very limited budgets might reasonably address their CIP-013 obligations.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation's position is that the determination of "cost effectiveness" will remain subjective unless a method to determine burden is consistent across the industry.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	

Answer	No
Document Name	
Comment	
There is not enough clarity in the proposed language to make that assessment.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro does not agree that implementing this standard will be cost effective. Costs and contract management to enforce CIP-013 on all vendors, in light of the limited authority the responsible entity would have over vendors, are anticipated to be significant. Especially, but not limited too, in situations where there is limited vendor choice for a class of product.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No

Document Name	
Comment	
The Implementation Guidance only identifies items that could be evaluated in developintg a Supply Chain Cyber Security program, but does not provide an example or guidance on how to implement the program. Without this guidance, it is impossible to understand how to comply with CIP-013-1 in a cost-effective and compliant manner.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Shawn Abrams - Santee Cooper - 1	
Answer	No
Document Name	
Comment	
Santee Cooper believes that this standard will increase the cost of purchasing products from vendors unless the standard effectively addresses the use of regional master contracts, master agreements, and piggyback agreements. If a Responsible Entity loses the ability to utilize such contracts and agreements the aggregated buying power and large purchase discounts will be lost.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No

Document Name	
Comment	
CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity. Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities. The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., "Each Responsible Entity shall <insert performance activity> and document the results of the assessment."). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	

By not clarifying “cyber security risks” in R1 Part 1.1 the SDT is not providing flexibility, but rather compliance risk to Registered Entities. See our comments to questions 1 and 7, above, regarding the Implementation Guidance. As it stands, the document provides no guidance and raises additional, possible compliance risk as to interpretation of what “cyber security risks” are.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity. Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities. The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall <insert performance activity> and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.	
Likes 0	

Dislikes 0	
Response. Thank you for your comments.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity.

Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall <insert performance activity> and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	

Answer	No
Document Name	
Comment	

CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity.

Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Richard Vine - California ISO - 2

Answer	Yes
Document Name	
Comment	

The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Avista agrees with the SDT's belief that the proposed CIP-013-1 and the ERO Enterprise-Endorsed Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. However, the cost effectiveness of the standard will ultimately depend on how Responsible Entities implement the standard and how NERC and the Regional Entities enforce the requirements. In addition to the Implementation Guidance, the policy guidance that NERC staff and the Standards Committee are drafting to clarify the principles, development, and use of the Guidelines and Technical Basis will also be very important to how Responsible Entities implement the requirements.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	

ERCOT joins the comments of the IRC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

No comment.	
Likes 0	
Dislikes 0	
Response	
Timothy Reyher - Eversource Energy - 5	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	

Dislikes 0	
Response. Thank you for your comments.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

We support the changes and believes that most aspects of CIP-013 may be achieved cost-effectively (if not necessarily cheaply), with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, USI strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. USI suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response. Thank you for your comments.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT's belief that the proposed CIP-013-1 and the ERO Enterprise-Endorsed Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. However, the cost effectiveness of the standard will ultimately depend on how Responsible Entities implement the standard and how NERC and the Regional Entities enforce the requirements. In addition to the Implementation Guidance, the policy guidance that NERC staff and the Standards Committee are drafting to clarify the principles, development, and use of the Guidelines and Technical Basis will also be very important to how Responsible Entities implement the requirements.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
In the Draft CIP-013-1 – Cyber Security - Supply Chain Risk Management requirement R2 includes the following: "Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract." With this note the Responsible Entity is basically directed to develop a plan yet it does not have to change procurement results. If you are not going to require results, there is no reason to add the costs of developing and implementing the program.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	

SDG&E is not able to determine if the proposed CIP-013-1 and the draft Implementation Guidance are cost effective. Additional changes to existing contracts could incur significant cost increases.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SRP generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, SRP strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BCS. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. SRP suggests that the option for a Technical Feasibility Exception be allowed for legacy

systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See attached comments.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE generally agrees the entities can meet the reliability objectives in a cost effective manner with two exceptions:	

(1) One exception is if the audit approach to CIP-013 effectively precludes use of regional master contracts and "piggyback" agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for: (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place of pre-negotiated master agreements, and (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, AE strongly urges that audit approach language for CIP-013 R2 be clarified to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors. (2) Implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BCS. Some legacy cyber systems are inherently structured and configured for vendor access and reworking them to allow real-time changes may degrade system performance. AE suggests the option for a Technical Feasibility Exception be allowed for legacy systems or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
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 generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, SMUD strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. SMUD suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill

Answer	Yes
Document Name	

Comment

SDG&E is not able to determine if the proposed CIP-013-1 and the draft Implementation Guidance are cost effective. Additional changes to existing contracts could incur significant cost increases.

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	

PRPA generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, PRPA strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. PRPA suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 0	
Dislikes 0	

Response. Thank you for your comments.	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
We support APPA's submitted comments regarding the cost-effectiveness of CIP-013, pointing out two exceptions.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	

Answer	Yes
Document Name	
Comment	
Note – Comments from EEI follow: "EEI agrees with the SDT's belief that the proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. However, the cost effectiveness of the standard will ultimately depend on how Responsible Entities implement the standard and how NERC and the Regional Entities enforce the requirements. In addition to the Implementation Guidance, the policy guidance that NERC staff and the Standards Committee are drafting to clarify the principles, development, and use of the Guidelines and Technical Basis will also be very important to how Responsible Entities implement the requirements. "	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
WECC concurs the draft of CIP-013-1 and the draft Implementation Guidance provide the flexibility sought by industry in its collective comments to the first ballot.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	

Answer	Yes
Document Name	
Comment	
Implementing action plans to meet reliability objectives should be cost effective, but cost effectiveness is different for each entity. Reasonable expectations of what's determined as "cost effectiveness" should be considered on an individual utility/entity basis.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
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	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
IESO	
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	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
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	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
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	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes

Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
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	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
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	
Answer	
Document Name	
Comment	
No comment	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	

Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Chris Scanlon - Exelon - 1	

Answer	
Document Name	
Comment	
At this point of the project, it is too early to comment on cost effectiveness. Exelon does not predict that the implementation of CIP-013 will require significant investment. However, implementing tools and processes for the revisions to CIP-005 and CIP-010 may require project management oversight as well as material financial investment.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

9. Provide any additional comments for the SDT to consider, if desired.
Mark Holman - PJM Interconnection, L.L.C. - 2
Answer
Document Name
Comment
The current version of the cybersecurity supply chain standard provides a starting point for advancing controls to mitigate the risks associated with vulnerabilities in the supply chain. PJM Interconnection, LLC ("PJM") is supportive of this proposed standard as a first step consistent with the overall direction provided by the FERC. *PJM wishes to point out that the proposed supply chain standard needs to further evolve through subsequent iterations based on additional experience and incorporation of best practices. Although PJM recognizes the limits of FERC's jurisdiction as it relates to*

suppliers to owners and operators of the bulk electric system, any effective supply chain management standard should work to create incentives for improved cybersecurity practices up the supply chain and not just place requirements on the end user (in this case the owner or operators of bulk electric system assets). Although not evident on its face, PJM is hopeful that the proposed Standard will adequately and timely incent that goal. However, as a first step, the impact of the proposed standard, once implemented, should be analyzed with this goal in mind.

In order for supply chain risks to be substantially mitigated it will require broader cross sector engagement, broad government engagement and a significant shift in how vendors and service providers deliver products and services. Broader engagement is also required to ensure an equitable allocation of liabilities and costs. Eventually vendors and service providers will differentiate themselves by how well they manage cybersecurity risks and meet these customer needs in a fair and responsible manner.

Directionally, the proposed cybersecurity supply chain standard was intended to address a broad range of technologies as opposed to a narrower view of Energy Management and Market Management System vendors. The FERC directive similarly appeared to drive this approach. By making this choice of applying the standard to a broader range of technologies the standard, almost by necessity, starts with a more general approach with is not overly prescriptive and is grounded on the principle that organizations must establish cybersecurity supply chain processes and then execute against those processes.

The standard could have been much more prescriptive had it taken a narrower approach focusing primarily on SCADA Systems, Energy Management Systems, and Market Management Systems software solutions. Clearly the more narrow approach would have allowed for additional focus on those systems most critical to ISO/RTO operations where more proscription could have been helpful to drive more specific cybersecurity controls up the supply chain. Whether a broad approach as chosen by the drafting team or a more targeted approach is better as a starting place can be legitimately debated. In any event, either can provide a starting point for making improvements in managing the cybersecurity supply chain threats. PJM believes this effort meets that initial 'out of the gate' requirement given the need for compliance with the FERC Order in a discrete time period.

Support of the cybersecurity supply chain standard will provide an incremental step in achieving our objective of significantly improving the risks associated with vulnerabilities in the supply chain.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	
Document Name	
Comment	
Luminant wants to thank the Supply Chain SDT for their diligence in reviewing the previous comments and using those comments to appropriately craft the current proposed documents. Luminant also wants to encourage the SDT to review the comments submitted during this ballot period and consider changes to the standards, as appropriate, even if these standards are passed by the ballot body.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes the proposed changes in the next posting are responsive to stakeholder comments, improve the quality of the standards, and meet the directives in Order No. 829.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Scott Downey - Peak Reliability - 1	
Answer	
Document Name	
Comment	
Peak Reliability believes the proposals are a step in the right direction but as written do not provide the value intended.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
1) Make 'vendor' a defined term or provide GTB explanation for what is expected to be considered a vendor. 2) Guidelines and Technical Basis for CIP-013-1 states that it is sufficient to establish a reliable software update source once to allow automated solutions to be implemented. Does this reasoning extend to manual patching? For non-automated systems can a reliable software update source be identified once? 3) Please provide implementation guidance on CIP-005 and CIP-010 4) Make 'integrity' a defined term or provide GTB explanation for what is expected for verifying integrity of software. 5) Please list practical ways to validate the integrity of software.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has addressed the comments in previous sections.	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	
Document Name	
Comment	
Make 'vendor' a defined term or provide GTB explanation for what is expected to be considered a vendor. Guidelines and Technical Basis for CIP-013-3 states that it is sufficient to establish a reliable software update source once to allow automated solutions to be implemented. Does this reasoning extend to manual patching? For non-automated systems can a reliable software update source be identified once? Please provide implementation guidance on CIP-005 and CIP-010 Make 'integrity' a defined term or provide GTB explanation for what is expected for verifying integrity of software. Please list practical ways to validate the integrity of software.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has addressed the comments in previous sections.	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	

Document Name	
Comment	
GRE appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Timothy Reyher - Eversource Energy - 5	
Answer	
Document Name	
Comment	
No Cooent	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	
Document Name	
Comment	

: The SDT doesn't address CIP Exceptional Circumstance (CEC) in any of the Supply Chain Standards. If an event does occur that creates a CEC, it could potentially cause an entity to not be able to monitor vendor remote access verification of software integrity and authenticity.

In Order No. 829, it states, "new or modified 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."

Does the drafting team have confidence that only having in scope medium and high BES Cyber Assets meets the directive for "industrial control system hardware, software, and services"?

ACES recommends additional verbiage be written in the requirements to document what cyber assets that are not in scope for Supply Chain Management such as: Electronic Access Control and Monitoring Systems (EACMS), transient cyber assets, removable media and protected cyber assets (PCA).

Thank you for your time and consideration.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT does not believe the proposed requirements need to include exceptions for CIP Exceptional Circumstances as discussed in previous sections.

The SDT believes the scope is appropriate, as discussed in response to Question 7.

The SDT does not believe it is necessary to expand on the list of exemptions; rather, the SDT has included the applicability in the appropriate section of the standard, and in the requirements themselves. This approach is consistent with other Reliability Standards.

Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	
Document Name	
Comment	
PSE supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	
Document Name	
Comment	
No comment	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	
Document Name	

Comment	
GTC appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	
The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches." The requirement wording suggests it applies for any change but the guidance suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the guidance is not, the guidance becomes superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. Therefore, the IRC suggest that either the requirement wording be adjusted to allow for automated patching solutions or the Guideline be removed as it is contradictory. The IRC suggest that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore the best solution is to remove the guideline.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the section in CIP-010-3 to remove the ambiguous material.	

IESO	
Answer	YES
Document Name	
Comment	

There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1.

The requirement states “For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5”.

The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

The requirement wording suggests it applies for any change but the guidance suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the guidance is not, the guidance becomes superfluous. The Guideline also introduces significant ambiguity that is impossible to audit.

Therefor the IESO suggest that either the requirement wording be adjusted to allow for automated patching solutions or the Guideline be removed as it is contradictory. The IESO suggest that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore the best solution is to remove the guideline.

Note: the following comment is the same as identified for question 2.

We note there is no corresponding “Guidance and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.

Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT has revised the section in CIP-010-3 to remove the ambiguous material. Also, see response in Question 2.	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
1. Make 'vendor' a defined term or provide GTB explanation for what is expected to be considered a vendor. 2. Guidelines and Technical Basis for CIP-013-3 states that it is sufficient to establish a reliable software update source once to allow automated solutions to be implemented. Does this reasoning extend to manual patching? For non-automated systems, can a reliable software update source be identified once? 3. Please provide implementation guidance on CIP-005 and CIP-010. 4. Make 'integrity' a defimed term or provide GTB explanation for what is expected for verifying integrity of software. 5. Please list practical ways to validate the integrity of software.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. See response in previous sections.	
William Harris - Foundation for Resilient Societies - 8	
Answer	

Document Name	Resilient Societies Comments - NERC Cyber Supply Chain Risk Management 2016-03.docx
Comment	
See combined comments of the Foundation for Resilient Societies in the attached file. (Comment at end of document)	
Likes 0	
Dislikes 0	

Response. Thank you for your comment.

1. The proposed standards will benefit reliability and enhance the existing body of CIP Reliability Standards by addressing supply chain cyber security risks to applicable medium and high impact BES Cyber Systems. The effort is in recognition of the significant and evolving threats to the cyber security of BES Cyber Systems in the supply chain. The proposed standards are responsive to FERC Order No. 829 and support a defense-in-depth strategy by adding planning and procurement obligations to "post-acquisition activities at individual entities" (Order No. 829, P. 34).
2. The proposed standards address the four supply chain cyber security objectives in Order No. 829 (software integrity and authenticity; vendor remote access; information system planning; and vendor risk management) through requirements for responsible entities to implement various planning and procurement processes and operating measures. Consistent with the Order, the proposed standards provide responsible entities with flexibility to determine how to meet the reliability objectives (Order No. 829, P. 2). Flexibility is needed due to the diverse population of responsible entities, the variety of systems and services covered by the standards, entity and vendor-specific procurement processes involved, and the evolving nature of cyber security supply chain risks and mitigation.
3. The proposed standards and Order No. 829 directing their development are informed by pertinent threat advisories and information (Order No. 829, P. 26). As discussed above, the proposed requirements provide entities with flexibility for achieving the objectives and avoid prescriptive measures that may not provide reliability benefits or deliver the most efficient or effective approach. Instead, the standards and Implementation Guidance reference current technical guidance where appropriate.
4. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. See response to Question 4 comments. Security of communications is not in scope for this project.

5. As discussed above, the proposed standards support a defense-in-depth strategy by adding planning and procurement obligations for responsible entities to other CIP cyber security practices. The SDT's approach is in line with FERC Order No. 829, which stipulates that the standards should not impose obligations directly on vendors (Order No. 829, P 36). 6. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. As a result, responsible entities have a vetted example of a compliant approach to support compliance monitoring activities. 7. Approved CIP standards contain requirements for mitigating malicious code and reporting cyber security incidents. Project 2016-03 is focused on the objectives contained in the project Standard Authorization Request and Order No. 829.

John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	

ERCOT joins the comments of the IRC and offers the following additional comment:

The term "vendor" that is used repeatedly in the rationale boxes requires further clarification or revision. "A *vendor*, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators."

Services cannot be manufactured, and the provision of services is already addressed through item (ii). ERCOT suggests the following revision: "A *vendor*, as used in the standard, may include: (i) developers or manufacturers of information systems or components; (ii) *providers of information systems services*; (iii) product resellers; or (iv) system integrators."

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT believes the vendor description as written provides responsible entities with the necessary context to meet the requirements.

Richard Vine - California ISO - 2

Answer	
Document Name	

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
Regarding requirement R2, measure M2, suggest consider revising language to state "…demonstrate use of ***or compliance with*** *the supply chain cyber security risk management plan."*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT does not believe the suggested change provides additional clarity.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	
Document Name	
Comment	
CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	
Document Name	
Comment	
CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	
Document Name	
Comment	
CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	
Document Name	
Comment	

Dominion recommends the following changes to the RSAWs:

- CIP-005-6, R2, Parts 2.4 and 2.5
  - Remove the word “all” from the “Compliance Assessment Approach sections.
- CIP-010-3, R1, Part 1.6
  - Remove the words “for each” from the “Compliance Assessment Approach section, rows 2 and 4.
- CIP-013-1, R1
  - Remove the word “controls”. The word “processes” is now in uses in the most current draft of CIP-013-1.

Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT will provide this feedback to the RSAW Task Force for consideration.	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	
Document Name	

Comment
CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

Patrick Hughes - National Electrical Manufacturers Association - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	NEMA Comments on NERC Supply Chain Risk Management 2017-06-12.pdf

Comment
On behalf of the National Electrical Manufacturers Association (NEMA)—a trade association and standards developing organization with nearly 350 member companies that manufacture a diverse set of products used in the generation, transmission, distribution, and end-use of electricity—and on behalf of the NEMA Grid Modernization Leadership Council and the NEMA Cybersecurity Committee, I wish to submit for your reference "CPSP 1-2015: Supply Chain Best Practices," which describes industry best practices for manufacturers to follow regarding cybersecurity supply chain management. "Supply Chain Best Practices" identifies guidelines that electrical equipment manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses or other exploits can be used can be used to negatively impact product operation. It addresses United States supply chain integrity through four phases of a product's life cycle: manufacturing, delivery, operation, and end-of-life. The report (attached) is available for public download at: http://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx.

The National Electrical Manufacturers Association and its members understand that a secure supply chain is essential to a secure grid and that cybersecurity aspects should be built into, not bolted onto, manufacturers' products. They also understand that managing cybersecurity supply chain risk requires a collaborative effort and open lines of communication among electric utility companies and the manufacturers of critical electric grid systems and components—both hardware and software. NEMA looks forward to working with and being a resource for NERC, utilities, and other interested stakeholders in addressing supply chain risks and concerns within the energy sector. Should you have any questions, please contact Patrick Hughes, Senior Director of Government Relations and Strategic Initiatives, at 703-841-3205 or patrick.hughes@nema.org. Respectfully, Kyle Pitsor Vice President, Government Relations	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	

Response	
Louis Guidry - Louis Guidry On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 3, 1; Michelle Corley, Cleco Corporation, 6, 5, 3, 1; Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; Stephanie Huffman, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	
Document Name	
Comment	
The Guidance and Techincal Basis section is empty.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. See the Implementation Guidance.	
Thomas Foltz - AEP - 5	
Answer	
Document Name	
Comment	
AEP urges the SDT to consider FERC Order 706 paragraph 355 which requires a policy for each of the cyber security topical areas. CIP-003 R1 should require a policy for supply chain cyber security.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT will provide this information to the CIP Modifications SDT.	

Tyson Archie - Platte River Power Authority - 5	
Answer	
Document Name	
Comment	
Platte River Power Authority also supports the comments submitted by the American Public Power Association (APPA)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
CenterPoint Energy appreciates the Standard Drafting Team's thorough consideration of comments. Although some concerns with implementation remain, CenterPoint Energy believes that the revisions have made the draft Standard focused and risk-based. CenterPoint Energy also commends the coordination with the CIP Modifications team to place certain requirements appropriately in the body of the existing CIP Standards. Thank you for your efforts.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Andrew Gallo - Austin Energy - 6	

Answer	
Document Name	
Comment	
None.	
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	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	
Document Name	
Comment	

No comment	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
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 members firms, numbering more than 5,000 and representing over 500,000 employees throughout the country, are engaged in a wide range of engineering work 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. ACEC is in agreement with most of the comments of the owners, operators, vendors and suppliers that have formally participated in this Standard development.

Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	
Comment	
NRECA appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI greatly appreciates the work of the SDT and NERC in reviewing and addressing stakeholder feedback from the first ballot. EEI supports the currently posted drafts and ask that the SDT look to our members' individual comments for further suggestions for improvement.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
David Rivera - New York Power Authority - 3	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	

Document Name	
Comment	
Please note that the NSRF has concerns with the Webinar and Guidance going outside of the scope of the proposed Requirements. All applicable entities will need to satisfy the Requirements once approved by FERC per FERC Order 693, setcion253. Regardless of what the Webinar or Guideline states.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	

Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
GSOC appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	

MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	

Additional comments received from Seattle City Light

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.

☒ Yes
☐ No

Comments: *Note that for all comments (1-9) written in blue text come directly from APPA and/or LPPC comments. Any comments in black are City Light's.*

Seattle City Light continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.

Seattle agrees with limiting the requirement to high and medium assets only.

R1: Seattle generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, might be included in the standard for these kinds of procurement activities. Alternatively, concerns about how different type of contracts—multi-party contracts, master agreements, evergreen agreements, piggyback contracts, long-term service agreements, etc, etc, etc—may or may not comply might be addressed by re-positioning CIP-013 as a performance-based Standard, with a focus on managing specific aspects of vendor security rather than particular contracting practices.

Our reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and (attempt to) achieve the protections identified in R1.2. It is immaterial how these protections are pursued. Focusing vendor security plans and audit approaches on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such we suggest that R1.2 be revised as follows:

> ***1.2.*** *One or more process(es) for its newly procured BES Cyber Systems that address the following elements, as applicable:*

As explanation for the revisions, underlined words are added, and "newly" is intended to mean 'obtained after the implementation of CIP-013.' Also, the term "elements," as shown above, is added to more clearly align with the VSLs for this requirement.

At the same time guidance associated with the "Rationale for R1," "Rationale for R2," and the separate Implementation Guidance document should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no necessary function in vendor security plans and audit approaches. Contract terms might be used by an entity in their vendor security plans and/or as evidence of performance, but there should be no expectation by auditors or subtext in the Standard or Implementation Guidance that anything having to do with contracts or procurement processes is required. There should be no expectation of what might or should be included within Requests for Proposals, no expectation of when contracts might or should be renegotiated, no expectations of what contract terms might or should be included or requested, and no expectations of what terms might or should be found in a prudent and proper contract. Ultimately there should be no expectation that CIP-013 R1.2 protections be achieved through the contracting process. Consistent with performance-based standard principles the objective in CIP-013 and in entity vendor security plans should be on achieving each protection (as feasible), not on the means by which it is achieved (or attempted to be achieved).

In the absence of such changes, we request substantial additional clarification about how, without contract terms and contract negotiations being auditable, performance of R2 implementation will be audited and assessed. In particular for state and regional master agreements, piggyback contracts, evergreen agreements, and the like.

Looking to specific details of CIP-013 requirements, Seattle requests re-wording of R1 parts 1.2.1 and 1.2.4 to better understand what is expected. These parts appear to be duplicative. The endorsed Guidance does not adequately distinguish between the two parts. One interpretation is that part 1.2.1 is for products/services and that part 1.2.4 is for vulnerabilities in the product. It is not clear if these parts expect information sharing at the time of procurement or if information sharing will be on-going?

In R1 parts 1.2.1 and 1.2.2, the term "vendor-identified incident" is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor, or incidents identified by the vendor. Seattle suggests changing "identified" in the phrase, to "acknowledged" or "confirmed" to ensure clarity.

Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005.

Seattle believes the SDT should provide guidance regarding the use of the term "vendor." If "Vendor" is not defined by NERC, the Guidance should recommend that entities include their definition of "vendor" in their plan(s).

Seattle recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

R2: Seattle agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in Requirement 1.

As discussed above, Seattle urges the significant additional guidance, preferably centered on performance-based principles, about expected compliance practices and how implementation will be audited. In particular for state and regional master agreements, piggyback contracts, evergreen agreements, and the like.

Finally, the Compliance and/or Implementation Guidance should make clear that, when evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

R3: Seattle agrees that a 15-month review period is appropriate to review the supply chain cyber security risk management plan in Requirement 1.

Additionally, Seattle proposes that the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date. This is similar to when the regional entities performed transition period audits of CIP v5 programs.

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the 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. The SDT followed

an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

☒ Yes
☐ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

The proposed CIP-005-6 uses the term, "vendor." The definition of vendor is not a NERC defined term. Seattle City Light believes the SDT should provide guidance regarding the use of the term "vendor." If "Vendor" is not defined by NERC, the Guidance should recommend that Entities include their definition of "vendor" in their plan(s).

Seattle agrees with R2 Part 2.4 but requests clarification of the term "determining."

Seattle generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective "is for entities to have the ability to rapidly disable active remote access sessions…" The Responsible Entity may not have the capability to disable access during an "active" remote access session. Seattle requests changing the language to "upon detected unauthorized activity."

Guideline & Technical Basis (GTB) for R2 should be included in this revision. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Please Include reference to FERC Order 829 for parts 2.4 and 2.5.

The SDT should consider adding a CIP Exceptional Circumstance clause to R2 parts 2.4 and 2.5

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 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). The SDT followed an approach recommended by stakeholders

during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.

☒ Yes
☐ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light agrees this requirement belongs in CIP-010 R1. Seattle generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- Seattle recommends the Guidelines and Technical Basis section is updated to reflect current information.
  - The requirement states "For a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5…," indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."
  - Seattle also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.
- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third-party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed, in particular for R1.6.1 and R1.6.2. Additionally, Seattle requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While Seattle supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to

deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and minimize audit challenges.

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT's removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

☒ Yes
☐ No

Comments: Seattle City Light agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. Among other things, the Order requests a risk-based approach. Application of Standard CIP-002 is an established, Commission-approved approach to categorize a utility's BES Cyber Systems into high, medium, and low risk classifications. Application of this established risk-based approach to cyber asset procurement for electric utilities is natural, appropriate, and consistent with the guiding CIP philosophy, stated in Section 6 of each CIP Standard, that each Standard "exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems."

Furthermore, Seattle believes that for entities that have a mixture of High, Medium and Low assets, the Low assets would inherently benefit from the additional requirements of Medium and High requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have Low assets only, there would not be additional requirements based on CIP-002 risk based approach, as appropriate to the low BES risk presented by these entities.

Seattle believes that including Lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items, beyond the benefit provided by additional controls. Existing controls inherent to CIP-003 and previous CIP Standards reduce the risk associated with Lows.

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.

☒ Yes
☐ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. Seattle feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers.

Seattle, in line with our recommendation to move CIP-013 to a performance-based standard as discussed in Question 1 above, also recommends deleting discussion of contracts and contract dates from implementation guidance, and focusing the guidance on BES Cyber Assets procured subsequent to the implementation date of the standard. If performance-based principles are not adopted, Seattle at least asks for clarity to change this General Consideration from:

> *Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.*

To:

> *Supply Chain Risk Management plan must be used by appropriate procurement processes that begin on or after the implementation date.* (Also make corresponding change to the associated note in CIP-013 R2.)

Further, Seattle requests clarification on if/when existing contracts, master contracts, or long-term maintenance agreements that may be re-opened for renegotiation or later put in use (e.g., a state master contract negotiated prior to the CIP-013 implementation date but not actually used by a utility until after CIP-013 implementation date), come into the scope of CIP-013. Seattle notes that shifting to a performance-based Standard, focused on specific vendor protections and not the means that such protections are achieved (i.e., contracts) would minimize the explanations required about such matters.

The Implementation Plan does not handle unplanned changes such as newly identified IROLs or registration changes, etc, that may bring an entity suddenly into scope for CIP-013, CIP-005 R2.4-2.5, and/or CIP-010 R1.6. Seattle therefore requests that the Implementation Plan be modified to address, in a reasonable way, how entities come into compliance if, due to changes, they newly meet applicability at some time after the effective date of the standards.

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.

☐ Yes
☒ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light agrees with the VRFs and VSLs for CIP-013. As discussed above under Question 1, Seattle requests that the term "elements" be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement.

For CIP-010, Seattle does not find that the VSL covers failures to implement the process. It therefore does not include all possible combinations of violation. Consequently, we request that there be an identified severity level for failure to implement and lower severity levels when a single aspect of the requirements is missing.

For CIP-005, Seattle believes that the VRFs and VSLs should be updated to reflect the same general structure used in CIP-010. The VSL for CIP-005 results in a "Severe" penalty if the entity did not have a method to determine and did not have a method to disable. Seattle would prefer a "High" VSL penalty if the entity has a process to determine but does not have a process to disable, and vice-versa if the entity did not have a process to determine but does have a process to disable.

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on

Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

☐ Yes
☒ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. Seattle is concerned about the possibilities that NERC and the Regions may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, Seattle would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard, including for CIP-005-6 R2.4 and R2.5 and for CIP-010-3 R1.6.

As discussed above, "vendor" is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005. Seattle believes the SDT should provide guidance regarding the use of the term "vendor." If "vendor" is not defined by NERC, the Guidance should recommend that entities include their definition of "vendor" in their plan(s).

Neither of the bullets for R3 in the Implementation Guidance sufficiently explain compliance needs because both bullets only deal with plan review and not approval, both of which are necessary for compliance. Therefore, Seattle recommends changing:

"Below are some examples of approaches to comply with this requirement:"

to

"Below is an example of an approach to comply with the review requirement required by: "

In addition, we recommend deleting the following guidance language from the second main bullet, because it is beyond the Requirement and introduced activities that are not explicitly required:

"Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed."

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

☒ Yes
☐ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if that if, due to uncertainty, anticipated audit risk, an eventually established audit approach, or any other reason, Standard CIP-013 precludes or has a chilling effect on use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other publics with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually to replace pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, Seattle strongly urges that audit approach language for CIP-013 R2 be clarified in advance to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions, auditors, time, and chance.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. Seattle suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or alternatively that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

9. Provide any additional comments for the SDT to consider, if desired.
Comments: None

End of Seattle City Light Comments

THE FOUNDATION FOR RESILIENT SOCIETIES COMMENTS AS FOLLOWS *ON PROPOSED STANDARD*
2016-03, CYBER SUPPLY CHAIN RISK MANAGEMENT, CIP-005-6, CIP-010-3, AND CIP-013-1:
Filed with NERC June 15, 2017
1. These NERC/SDT attempts to produce a CIP standard for supply chain vulnerabilities fall short in an extreme threat environment. Adversaries' efforts against the electric grid and other civil infrastructure show disdain for U.S. defenses and deep commitment to using Information Operations (including cyber warfare) against the nation. The Bulk Electric System (BES) is a major target—this motivates development of strong capabilities for cyberattack. Adversaries understand full well the dependencies of social and national security institutions and all other critical infrastructures on electric power.

2. There is insufficient substance to the draft standard, other than the usual CIP generalized statements of planning, implementation, and periodic reviews that provide *pro forma* response to FERC Order No. 829. In its 9-1 vote to reject the first draft, the industry sent a clear message to NERC and FERC: the standard requirements are, at present, inadequately defined and therefore the feasibility of cost recovery is hard to judge.

3. Any sincere attempt at compliance with the draft standard requirements by responsible entities will incur high costs with uncertain benefit to the survivability of the BES. The Standard Drafting Team appears to minimize the complexity of the 2014 Russian penetrations of the U.S. BES, its sophisticated multi-layered, years-earlier penetration of vendor's control systems, phishing efforts, firmware modifications, and extensive use of IT vendors' vulnerabilities in operating, communications and networking, and database systems. The draft lacks good protective steps on these vulnerabilities and is therefore inadequate for mitigating risk--especially given the increasing nature of the Russian Havex and BlackEnergy threats evidenced in the follow-on attacks in the Ukraine Grid in 2015 and 2016. Note the recent revelation by ESET and DRAGOS of CRASH OVERIDE malware (associated with the 2016 Ukraine attack) with specific and flexible targeting of "low impact" industrial control systems (ICS). Note also the increasing threat from Distributed Denial of Service (DDoS) IoT and ransomware attacks. To expect several thousand utilities to individually and separately determine self-protective actions under the draft standard is unrealistic. Economies of scale in protection are needed.

4. Exempting "Low Impact" cyber systems leaves vulnerabilities. Also, as Resilient Societies has pointed out on FERC dockets, the exclusion from CIP Standards for all communications and networks between "Electronic Security Perimeters," together with direct internet connectivity to many so-called "low impact" cyber assets, leaves literally thousands of unsecured channels for malware implantation.

5. Stringent application whitelisting/blacklisting and selective third party certification steps, in conjunction with a national deterrence policy, are needed to enhance the minimal-protection from current CIP standards.

6. Ambiguities in standard requirements result in a lack of auditability, as noted by many other commenters.

7. In the short-term, a more practical NERC initiative could be to support a FERC rulemaking to require Bulk Electric System-jurisdictional entities to detect, report, mitigate and remove malware. State PUCs should likewise support a malware mitigation initiative for distribution utilities.

William R. Harris
Foundation for Resilient Societies, Inc.

End of Report