Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Technical Rationale and Justification for CIP-012-1
Comment Period Start Date:	8/14/2017
Comment Period End Date:	9/12/2017
Associated Ballots:	

There were 42 sets of responses, including comments from approximately 137 different people from approximately 92 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT developed draft Technical Rationale and Justification for CIP-012-1 to provide stakeholders and the ERO Enterprise an understanding of the technology and technical requirements in the Reliability Standard. Do you agree that the draft Technical Rationale and Justification for CIP-012-1 clearly explains the technical reasoning for the proposed standard? If you do not agree, or if you agree but have comments or suggestions for the draft document, please provide your recommendation and explanation.

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	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	FRCC,MRO,NPCC,SERC,SPP RE,Texas RE,WECC	Southern Company	Katherine Prewitt	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company - Southern Company Generation	5	SERC
					Jennifer Sykes	Southern Company - Southern Company Generation and Energy Marketing	6	SERC
Florida Municipal Power Agency	Brandon McCormick	3,4,5	FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC

					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Midcontinent ISO, Inc.	David Francis	2,3	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
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC

					Matt Goldberg	ISONE	2	NPCC
SERC Reliability Corporation	David Greene	10	SERC	SERC CIPC	Bill Peterson	SERC RRO	10	SERC
					Mike Hagee	SERC RRO	10	SERC
					SERC CIPC	Various	1,2,5,9	SERC
Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	1,3,5,6	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
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
Santee Cooper	James Poston	1,3,5,6		Santee Cooper	Rene' Free	Santee Cooper	1	SERC
					Rodger Blakely	Santee Cooper	1	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC
					Tom Abrams	Santee Cooper	1	SERC
					Jennifer Richards	Santee Cooper	1	SERC
					Stony Martin	Santee Cooper	1	SERC
					Glenn Stephens	Santee Cooper	1	SERC
					Tom Perry	Santee Cooper	1	SERC
	Patricia Robertson	1,3,5		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC

BC Hydro and Power Authority					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 Con-Edison and Dominion	Guy V. Zito	Northeast Power Coordinating Council	10	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Laura Mcleod	NB Power	1	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Greg Campoli	NYISO	2	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC

					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Helen Lainis	IESO	2	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Deborah McEndaffer	Midwest Energy, Inc.	NA - Not Applicable	SPP RE
					Don Schmit	Nebraska Public Power District	5	SPP RE
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Hirchak	Cleco Corporation	6	SPP RE
					Marty Paulk	Cleco Corporation	1,3,5,6	SPP RE
					Michelle Corley	Cleco Corporation	3	SPP RE
					Robert Gray	Board of Public Utilities	NA - Not Applicable	SPP RE
					Ron Spicer	EDP Renewables	NA - Not Applicable	SPP RE
					Steven Keller	Southwest Power Pool	2	SPP RE
					Laura Cox	Westar Energy	5	SPP RE
PPL - Louisville Gas and Electric Co.	Shelby Wade	3,5,6	RF,SERC	Louisville Gas and Electric Company and Kentucky Utilities Company	Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					Dan Wilson	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
PSEG	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF
					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF

					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF

1. The SDT developed draft Technical Rationale and Justification for CIP-012-1 to provide stakeholders and the ERO Enterprise an understanding of the technology and technical requirements in the Reliability Standard. Do you agree that the draft Technical Rationale and Justification for CIP-012-1 clearly explains the technical reasoning for the proposed standard? If you do not agree, or if you agree but have comments or suggestions for the draft document, please provide your recommendation and explanation.

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

The IESO offers the following comments:

- On page 5, under the Control Center Ownership section, the following statement is confusing, “Applying protection among a Responsible Entity’s owned Control Centers is solely at its discretion.” Our understanding is that choosing to apply protections is not at our discretion, it is required. We recommend the following, “The method of applying protection to Control Center’s exclusively owned by a Responsible Entity is solely at its discretion. However, when multiple Responsible Entities own a Control Center at either end of the communication link, applying protection requires additional coordination and diligence.”
- Recommend that the rationale state that the standard does not increase the scope of BES Cyber Systems that require protections under CIP-002 thru CIP-011. The requirements apply only to the protection of the data that is transmitted across infrastructure not owned by a Responsible Entity.
- Implementation guidance is needed on the use of armored cable as a physical security protection method when using leased or subscribed fiber with multiple telecom carriers in the path. The guidance needs to address router hops and fiber patch panels that exist within a telecom provider’s central office.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison

Answer	No
Document Name	

Comment

Please disregard answer above. This was an error. I am unable to change it. We have no comments on this item. Dermot Smyth.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 1,3,5,6	
Answer	No
Document Name	
Comment	
While the CIP standards should emphasize outcomes and allow entities to achieve specific security objectives in many ways, protections applied to communications should be evaluated with due consideration of the context in which people, processes and technology are applied to establish a given security protection. Demonstration of risk mitigation should include assessment of not just technology and process to provide protection, but also the diversity and severity of threats present in a given context (e.g. the difference between dedicated communication links as opposed to broadly shared communications infrastructure). Particular technology and process applied in a context with fewer or lower likelihood threats should be preferred over the same technology and process in a context with more or greater likelihood threats (i.e. greater overall risk). Simply specifying that some (how much?) risk mitigation should be applied by means that include physical, logical and possibly other means leads to insufficient conditions for establishing compliance both for the responsible entity and anyone reviewing compliance for that entity. Entities should consider not only that risk mitigation should take place, but also the thresholds for residual risk that should be considered acceptable for such communication.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Florida Municipal Power Agency - 3,4,5 - FRCC, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA does not agree that the Technical Rationale and Justification for CIP-012-1 fully explains the technical reasoning for the standard. The Rationale document does not provide justification for the Operational Planning and Analysis data that is included in the scope of this standard. While the document does provide an example of communication paths (page 5), the example would be improved by adding a communication path between the TOP Control Center and the GOP Control Center.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	

Comment
SCL supports APPA comments

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5,6	
Answer	No
Document Name	

Comment
This document does not provide justification for the inclusion of the Operational Planning and Analysis data. NCPA suggests it be removed from the standards scope.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	

Comment
AZPS provides the following comments for the SDT's consideration: 1. The statement provided in "General Considerations for Requirement R1" clearly limits the applicability of Requirement R1 to the real-time horizon and does not indicate Requirement R1 being applicable to the Operational Planning Horizon. Specifically, the technical justification states that the focus is on "developing a plan to protect information that is critical to the real-time operations of the Bulk Electric System." This is in direct conflict with the draft standard, which scopes the plan to "to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data." AZPS reiterates its comments in response to the draft CIP-012-1 that the inclusion of data used for Operational Planning Analysis does not have a meaningful impact on reliability or real-time operations for the BES such that extending protection to Operational Planning Analysis results in overall benefits to reliability. 2. AZPS is concerned that the rationale provided in "Alignment with IRO and TOP standards" may misalign with the IRO Standards. The IRO and TOP Standards explicitly allow each responsible entity to develop individual data specifications because responsible entity processes can differ based upon operational characteristics, coordinated functional registrations, delegation agreements, operating agreements, etc. Statements within that section that these requirements force consistency in data and data specifications appear to directly conflict with the intent and flexibility of the IRO and TOP data specification requirements. 3. AZPS also suggests revising the third sentence in the section entitled "Control Center Ownership" because that sentence, read alone, absolves a responsible entity from protecting communications between its own control centers. The sentence in question reads "Applying protection

among a Responsible Entity's owned Control Centers is solely at its discretion." This sentence also seems to conflict with the first sentence in the same section.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
The document makes a good case for the security needed for Real-time data. It does not treat the Planning and Analysis data as well. Please see the AEP comments in the Unofficial Comment Form for CIP-012-1.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	Project 2016-02_CIP-012-1_NSRF Final.docx
Comment	
WAPA feels there is additional need for clarity and proposed language as identified in the NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Russell Noble - Cowlitz County PUD - 3,5	
Answer	No
Document Name	
Comment	
Cowlitz PUD supports comment submitted by APPA.	

Likes 0	
Dislikes 0	

Response

David Francis - Midcontinent ISO, Inc. - 2,3 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

The SRC & ITC SWG offers the following comments:

On page 5, under the Control Center Ownership section, the following statement is confusing, “Applying protection among a Responsible Entity’s owned Control Centers is solely at its discretion.” Our understanding is that choosing to apply protections is not at our discretion, it is required. We recommend the following, “The method of applying protection to Control Center’s exclusively owned by a Responsible Entity is solely at its discretion. However, when multiple Responsible Entities own a Control Center at either end of the communication link, applying protection requires additional coordination and diligence.”

Recommend that the rationale state that the standard does not increase the scope of BES Cyber Systems that require protections under CIP-002 thru CIP-011. The requirements apply only to the protection of the data that is transmitted across infrastructure not owned by a Responsible Entity.

Implementation guidance is needed on the use of armored cable as a physical security protection method when using leased or subscribed fiber with multiple telecom carriers in the path. The guidance needs to address router hops and fiber patch panels that exist within a telecom provider’s central office.

Likes 0	
Dislikes 0	

Response

Michael Puscas - ISO New England, Inc. - 2

Answer	No
Document Name	

Comment

In order to evaluate the extent and kind of obligation involved, the definition of between control centers needs to be clearer with regard to the communication link. What are the demarcation points for obligation to show compliance? Should there be explicit agreements with each end of the communication link to arrange such demarcation? How should responsible entities deal with third parties involved with trust relationships in communication links (i.e. telecommunications providers managing routers)?

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

A) It is understood that the reference model shown on page 5 is an example of communication paths. Suggest adding the communication path between the TOP Control Center and the GOP Control Center to provide further clarity.

B) This document does not provide justification for the inclusion of the Operational Planning and Analysis data is included in the scope of this standard. Suggest that this be added to the Technical Rationale and Justification document or this data be removed from the scope of the standard.

Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT ISO supports the comments of the ITC SWG.

The ITC SWG offers the following comments:

- On page 5, under the Control Center Ownership section, the following statement is confusing, “Applying protection among a Responsible Entity’s owned Control Centers is solely at its discretion.” Our understanding is that choosing to apply protections is not at our discretion, it is required. We recommend the following, “The method of applying protection to Control Center’s exclusively owned by a Responsible Entity is solely at its discretion. However, when multiple Responsible Entities own a Control Center at either end of the communication link, applying protection requires additional coordination and diligence.”

- Recommend that the rationale state that the standard does not increase the scope of BES Cyber Systems that require protections under CIP-002 thru CIP-011. The requirements apply only to the protection of the data that is transmitted across infrastructure not owned by a Responsible Entity.

- Implementation guidance is needed on the use of armored cable as a physical security protection method when using leased or subscribed fiber with multiple telecom carriers in the path. The guidance needs to address router hops and fiber patch panels that exist within a telecom provider's central office.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The SPP Standards Review Group recommends that the drafting team includes other Standards that are identified in question #2 comment form (Glossary of Terms Used in NERC Reliability Standards-Control Center). From our perspective, the technical documents only mention the applicable TOP and IRO Standards. If other standards are identified that are potentially impacted by this definition change, they need to be included in that the documentation to help support justification as well as showing consistency.

Likes 1	Stephanie Burns, N/A, Burns Stephanie
Dislikes 0	

Response

James Gower - Entergy - NA - Not Applicable - SERC

Answer	No
Document Name	

Comment

The standard as drafted explicitly excludes oral communications, but does not consider forms of written communication (email, chat, etc) that could communicate the same type of information that an oral communication could. These written instructions are commonly outside of SCADA systems and are on corporate systems, and this standard would require physical or logical controls on those systems for communications that may traverse these systems. The standard should specify the protection of "operational data", "BCS Data", or some other term to clarify protection of data outside of instructions, or provide data validation (i.e verify emails by phone) as an acceptable control.

Additionally, Entergy has concerns over expanding the scope of protection from "real-time" as defined in other CIP standards and through existing CIP definitions, to require the protection of Operational Planning Analysis data that is outside of the "real-time" horizon.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recommends the NIST definitions of “confidentiality” and “integrity” be added to the NERC Glossary of Terms Used in Reliability Standards, rather than referring to NIST Special Publication 800-53A, Revision 4.

Reclamation also recommends the Drafting Team state clearly that examples provided in Technical Rationale and Justification documents are neither mandatory, nor enforceable, nor the only method of achieving compliance.

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 Con-Edison and Dominion

Answer	No
Document Name	

Comment

While the CIP standards should emphasize outcomes, and allow entities to achieve specific security objectives in many ways, protections applied to communications should be evaluated with due consideration of the context in which people, processes and technology are applied to establish a given security protection. Demonstration of risk mitigation should include assessment of not just technology and process to provide protection, but also the diversity and severity of threats present in a given context (e.g. the difference between dedicated communication links as opposed to broadly shared communications infrastructure). Particular technology and process applied in a context with fewer or lower likelihood threats should be preferred over the same technology and process in a context with more or greater likelihood threats (i.e. greater overall risk). Simply specifying that some (how much?) risk mitigation should be applied by means that include physical, logical and possibly other means leads to insufficient conditions for establishing compliance both for the responsible entity and anyone reviewing compliance for that entity. Entities should consider not only that risk mitigation should take place, but also the thresholds for residual risk that should be considered acceptable for such communication.

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	

Comment

This document does not address what equally effective methods are or what appropriate physical controls may be. It also does not discuss where physical controls may or may not be appropriate over logical controls such as encryption. SRP also does not believe the document addresses latency or computer resource concerns. SRP requests additional guidance on what would be acceptable for these items.

SRP also agrees with APPA's recommendation to provide justification for the inclusion of the Operational Planning and Analysis data in the scope of this standard.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern disagrees with the Technical Rationale and Justification for CIP-012 for several reasons. We feel that the "data centric approach" being pursued opens the door for misinterpretation and the unintentional scoping-in of data that does not require protection. We are concerned that under the proposed Standard, the efforts required in redefining the data to be protected will obscure the true intent of the standard which is to protect the communications links over which the data travels. We feel that clarification of the scope of the data to be protected is essential for ensuring that the correct communications links are secured and the standard can be properly implemented via an appropriate technical solution. As currently written, Southern feels that the scope is too broad and the protections required would be cost prohibitive.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	

Comment

APPA does not agree that the Technical Rationale and Justification for CIP-012-1 fully explains the technical reasoning for the standard. The document does not address what equally effective methods are, or what appropriate physical controls may be. Nor does it discuss where physical controls may or may not be appropriate over logical controls such as encryption. In addition, latency and computer resource concerns are not addressed.

The Rationale document does not provide justification for the Operational Planning and Analysis data that is included in the scope of this standard.

While the document does provide an example of communication paths (page 5), the example would be improved by adding a communication path between the TOP Control Center and the GOP Control Center.

Likes 0	
Dislikes 0	

Response

Annette Johnston - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

MidAmerican Energy Company comments on the CIP-012 focused on two major areas which impact the Technical Rationale and Justification document.

One,we do not agree with two separate requirements, one for a plan and one to implement. We recommend following precedent in the other CIP standards, for example, CIP-004 through CIP-011. The obligation can be accomplished with one requirement,

Two, the scoping for sensitive data should be explicitly to information exchanged between Control Centers' BES Cyber Systems. This corresponds to SDT's assertation that "this data resides within BES Cyber Systems, and while at rest is protected by CIP-003 through CIP-011." It also corresponds to FERC's recognition in their order that certain entities are already required to exchange necessary real-time and operational planning data through secured networks using mutually agreeable security protocol.

Additionally, the Technical Rationale and Justification document creates a higher bar than the obligation in the requirement and should be changed. Specifically, expectation levels are different between the requirement “to mitigate the risk of the unauthorized disclosure or modification of data” and Technical Rationale and Justification's second sentence in the General Consideration for R2 section on page six, which states, “The protection must prevent unauthorized disclosure or modification of applicable data”. “Must prevent” is a higher bar than “mitigate the risk of.” The sentence on page 6 should be changed to match the sentence in the requirement.

MidAmerican Energy Company's comments on the proposed Control Center definition reflect concerns that renewable generation resources such as wind and solar are insufficiently addressed. While the concept of alignment with PER-005-2 has merit, PER-005-2 is antiquated in the reference to "plant operators located at a generator plant site." Renewable resources do not fit the traditional "plant site" or "plant operators" model of historical traditional generating plants. (The diagram on page five represents these as "control rooms." We agree with excluding the plant operators at the plant site for traditional generation. It must also be clear that the operating personnel at wind and solar farms are also excluded.

Corresponding to the comment above, the diagram on page 5 of the Technical Rationale and Justification should include a box to demonstrate with a red dashed line that renewables operating personnel are also out-of-scope for Control Center communications.

Also in the diagram, we are trying to understand the two BA Control Center boxes. Why does one have no field assets depicted?

Also in the diagram, there is a box for "GOP control room." Shouldn't this be labeled as a GO control room?

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6

Answer	No
Document Name	

Comment

Tacoma Power supports the comments of APPA.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC

Answer	Yes
Document Name	

Comment

However we are concerned because unauthorized alteration Operational Planning Analysis data does not pose a threat to the BES. This should be addressed by TOP 010-1 regarding the quality of the data. Accordingly, we are not clear on the utility of the standard since TOP 010-1 will mitigate the risk. Operational Planning Data is not real time data.

The SDT should consider exempting Email as they did with oral communication because of its use for communicating Operational Planning Data. We suggest that the SDT communicate the risk related to operational planning analysis data.

We would also like more guidance on key management and inter utility agreements on key management. Whatever measures implemented to meet compliance, it would increase operational burden and decrease reliability.

It may be more cost effective if an industry wide initiative is conducted with encryption specifications. There may be issues with entities using divergent technologies and measures to prevent an uncoordinated mismatched implementation that should be addressed. This initiative requires an industry wide standard, entities cannot decide individually to implement encryption schemes without coordination.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

OPG understands the focus is on protection of data communication between control centers but would like to clarify that it is not being required to verify integrity of data from it's origination points to the point where it's first aggregated at a control center, as this would be a substantially more difficult and costly requirement to achieve.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

While BPA agrees that the draft Technical Rationale and Justification for CIP-012-1 clearly explains the technical reasoning for the proposed standard, BPA does not agree that the intent of FERC Order No. 822 has been met. Order No. 822 requires implementation of controls to protect, at a minimum,

communication links AND sensitive BES data communicated between BES Control Centers. However, the SDT is providing latitude to protect communication links, data or both. BPA recommends placing controls on the data (encryption where availability requirements are not negatively impacted) AND end points (physical controls) where technically feasible.

Additionally, BPA has concerns about the SDT's assumption that "availability" is adequately addressed by other NERC standards (TOP-001-4 and IRO-002-5), as discussed in the "Overview of confidentiality and integrity" section of the Technical Rationale and Justification.

1. The proposed language includes protection of "confidentiality and integrity of data" but excludes "availability" from the language of the requirement. However, in the Confidentiality/Integrity/Availability (CIA) triad for information security, each leg must be balanced against the other two legs. By segregating Availability to TOP-001-4 and IRO-002-5, while leaving Confidentiality/Integrity in the proposed CIP-012 standard, it becomes impossible to properly balance all three legs of the triad to achieve optimum Reliability of the BES. The cyber security triad represents design tradeoffs; entities can't properly design communications networks – or worse: existing infrastructure may need to be rebuilt – if one of the options (Availability) is removed from consideration.

2. While TOP-001-4 and IRO-002-5 (redundancy and diverse routing of data) can be used to increase Availability, Availability can also be achieved through other equally effective methods. Therefore, "Availability" is not adequately addressed by TOP-001-4 and IRO-002-5 and limits entities' options to address availability by other methods more appropriate to their systems.

Therefore, BPA proposes that "availability" be included in the Technical Rationale and Justification to meet the security objectives of Order 822, i.e., "…to protect AVAILABILITY, confidentiality and integrity of data required for reliable operation...."

BPA also encourages the SDT to use the Guidelines and Technical Basis section to recognize the distinction between the engineering/design term "availability" (in which availability is quantitative – e.g., a system is designed to be available 99.99% of the time) and the cyber security application in which availability is a qualitative element of security that is constantly balanced against two other (often competing) elements (confidentiality and integrity).

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Poston - Santee Cooper - 1,3,5,6, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 3,5,6 - SERC, Group Name Louisville Gas and Electric Company and Kentucky Utilities Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Theresa Rakowsky - Puget Sound Energy, Inc. - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
David Greene - SERC Reliability Corporation - 10, Group Name SERC CIPC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - PSEG - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 3	PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4, Group Name FirstEnergy Corporation	
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	
Patricia Robertson - BC Hydro and Power Authority - 1,3,5, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the Security Working Group (SWG).	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE understands that the intent of a Technical Rationale document, as presented to the NERC Members Representative Committee on August 9, 2017, is to provide stakeholders and the ERO Enterprise an understanding of the technology and technical requirements of the Reliability Standard. However, the majority of this Technical Rationale Document for proposed Reliability Standard CIP-012-1 appear to be Implementation Guidance. Texas RE recommends following the process for submitting Implementation Guidance for the content of this document. Texas RE addressed its concerns with CIP-012-1 in its comments on the requirement language. Please refer to Texas RE's comments on the proposed draft of CIP-012-1. If, in the future, a draft Implementation Guidance is posted for review, Texas RE will evaluate it at that point.	

Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
N/A,	
Likes 0	
Dislikes 0	
Response	

Comments from Sean Erickson, WAPA

Questions

1. Requirement R1: The SDT drafted CIP-012-1 Requirement R1 to meet the mandatory requirement for the Responsible Entity to develop one or more documented plan(s) to mitigate the risk of the unauthorized disclosure or modification of data used for Operational Planning Analysis, Real-time Assessment, and Real-time monitoring data while being transmitted between Control Centers. Do you agree with this revision? If not, please provide the basis for your disagreement and an alternate proposal.

   ☐ Yes

   ☒ No

   Comments: As mentioned by the SDT, FERC directs *that "…require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers…"*. First, having a plan does not add to the reliability of protecting said data. This is an unwarranted layer of compliance that is not needed. Everything does not need a plan in order to be protected. Recommend that R1 be written in parallel to the FERC directive, which does not require a plan (per the SDTs Consideration of Issues and Directives).

   If "Plan" is maintained in CIP-012-1 then, the SDT should explain what is meant by having a Plan? Per CIP-003-6 it states, The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan

can describe an approach involving multiple procedures to address a broad subject matter. Is a plan the template document which is used throughout our Standards or is it a set of controls that show that the data is being protected per R1? The NSRF does not understand why a Plan is needed when the data is being protected by physical or electronic means. If a Plan is required, then all the Plan is going to say is that the cabling that transfers data is in a protected conduit (or other means) between Control Centers.

Secondly, The NSRF questions why the SDT is not in line with the FERC Order to "…protect …data…" but the proposed R1 states to "…mitigate the risk of unauthorized discloser or modification of data…"?

R1 should be rewritten to state: "The responsible entity shall have controls (or other understandable words) in place to protect against the unauthorized disclosure or modification of BES data used for Operational Planning Analysis, Real-time Assessments, and Real-time monitoring while being transmitted between BES Control Centers. This excludes oral communications". Please note that the word "BES" is needed within R1 regardless of it our proposed rewrite is accepted or not.

2. Requirement R1: The SDT seeks comment on the need to scope sensitive BES data as it applies to Operational Planning Analysis, Real-time Assessment, and Real-time monitoring. Do you agree with scoping CIP-012-1 Requirement R1 in this manner? Please provide comment in support of your response.

   ☐ Yes

   ☒ No

   Comments: The SDT needs to add "BES" data into the language as recommended above in question 1.

3. Implementation Plan: The SDT revised the Implementation Plan such that the standard and NERC Glossary terms are effective the first day of the first calendar quarter that is twelve (12) calendar months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority. Do you agree with this proposal? If you agree with the proposed implementation time period, please note the actions you will take that require this amount of time to complete. If you think an alternate implementation time period is needed – shorter or longer - please propose an alternate implementation plan and provide a detailed explanation of actions and time needed to meet the implementation deadline.

   ☐ Yes

   ☒ No

   Comments: The 12 month time period may only work for Entities who are vertically intergraded. The flow of applicable BES data within CIP-012-1 can be viewed as a "spider web" of data transfer for large RC foot-prints. With this being said, there may be non-compliance issues when one side of the data transference is protected and the other side is not. The SDT should propose a phased in approach to protecting data. A five (5) year implementation plan will allow entities to fund these projects. This is especially import to small entities. Per the NERC Guidance concerning "Phase Implementation Plans with Completion Percentages (http://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP_Practice_Guide_Phased_Implementation_Completion_Percentages.pdf) please state that the CIP-012-1 does not fall under this guidance.

4. The SDT believes proposed CIP-012-1 provides 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 more cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

☒ Yes

☐ No

Comments: Thank you for adding the third bullet of R1.

5. If you have additional comments on the proposed CIP-012-1 – Cyber Security -- Communication Networks drafted in response to the FERC directive that you have **not** provided in response to the questions above, please provide them here.

Comments:

1. The NSRF questions the use of "Real-time monitoring" as an applicable object within R1. "Real-time" is defined as "present time as opposed to future time". Which our industry understands and without the word "monitoring" being defined, may lead to misinterpretation by responsible entities and CEAs, alike. The word "monitoring" may mean ALL monitoring of an entity's entire SCADA system. It should be the "monitoring" of BES data, only, that is required for Operational Planning Analysis and Real-time Assessments.

2. The Applicability section states, "For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly". This proposed Standard does not specify any specific entities and recommend that this be removed.

3. The NSRF has concerns with the proposed definition of Control Center. The largest issue is the last paragraph concerning a Generating Operator. The use of the word "capability" is ambiguous and will confuse Registered Entities and CEAs, a like. The SDT should consider the approved Applicability within PER-005-2 part 4.1.5.1, which reads:

Dispatch personnel at a centrally located dispatch center who receive direction from the Generator Operator's Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner, and may develop specific dispatch instructions for plant operators under their control. These personnel do not include plant operators located at a generator plant site or personnel at a centrally located dispatch center who relay dispatch instructions without making any modifications.

This aligns with current and understood wording of PER-005-2.

4. Are the noted "Real-time reliability related- tasks" within the proposed definition, the same "Real-time Reliability-related task prescribed in PER-005-2? If so, please state this in your consideration of comments document and within your guidance document.

5. The NSRF believes that data associated with Operational Planning Analyses (OPA), Real-time monitoring (RTm), and Real-time Assessments (RTA) are predicated on other Standards and protection of data is required but all three areas (OPA, RTm, and RTA) are not subject equally to the Applicable Entities noted in CIP-012-1. Per IRO-010-2, R1, the RC is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R1 the TOP is to document its specifications necessary for OPA, RTm, and RTA. Per TOP-003-3, R2, the BA is to document its

specifications necessary for analysis functions and RTm, only. The SDT, in the Technical Rationale and Justification document acknowledges TOP-003 and IRO-010 "provides consistent scoping of identified data" [R1 section: Alignment with IRO and TOP Standards"]. The SDT should quantify that the data to be protected is the data associated with the Applicable entities with IRO-010-2 and TOP-003-3. With doing this, the SDT will articulate what the entity is to preform what analysis and what "data" is to be protected, based on already approved NERC Reliability Standards. By clearly identifying (and linking) the data to be protected from the data specifications developed under Standards TOP-003 and IRO-010, there is no room for interpretation of what "data" is to be protected.