Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Technical Rationale and Justification and Implementation Guidance for CIP-012-1
Comment Period Start Date:	11/20/2017
Comment Period End Date:	12/11/2017
Associated Ballots:	

There were 30 sets of responses, including comments from approximately 84 different people from approximately 59 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 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

2. The SDT developed draft Implementation Guidance for CIP-012 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.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
SRC & SWG	David Francis	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
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC
					Matt Goldberg	ISONE	2	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

Public Utility District No. 1 of Chelan County	Janis Weddle	1,3,5,6		Chelan PUD	Haley Sousa	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Janis Weddle	Public Utility District No. 1 of Chelan County	6	WECC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion and ISO-NE	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

					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Paul Malozewski	Hydro One Networks, Inc.	3	NPCC
					Helen Lainis	IESO	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					Greg Campoli	NYISO	2	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Chantal Mazza	Hydro Quebec	2	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
					Michael Forte	Con Ed - Consolidated Edison	1	NPCC
					Daniel Grinkevich	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Brian O'Boyle	Con Ed - Consolidated Edison	5	NPCC
					Sean Cavote	PSEG	4	NPCC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Megan Wagner	Westar Energy	6	SPP RE
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Gray	Board of Public Utilities (BPU), Kansas City, KS	NA - Not Applicable	NA - Not Applicable

					Ron Spicer	EDF Renewables	5	SPP RE

1. The SDT developed draft Technical Rationale and Justification for CIP-012 to assist in understanding the technology and technical requirements in the Reliability Standard. It also contains information on the SDT's intent in drafting the requirements. Do you agree with the technology and technical requirements in the draft Technical Rationale and Justification? If you do not agree, or if you agree but have comments or suggestions for the draft Technical Rationale and Justification, please provide your recommendation and explanation.

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD

Answer	No
Document Name	

Comment

The technical guidance sections do a suitable job of describing the problem that the SDT is being asked to solve. The rationale for the alignment, however, introduces concern given that the term "Real-time monitoring", while aligned with IRO and TOP terminology, is not itself a NERC-defined term and is also being further modified to create another new "Real-time monitoring and control" undefined term. Given that the term is already being changed, CHPD requests that the STD instead consider creating a new "BES data" (a term used by the SDT in the Draft 2 Unofficial Comment Form) NERC Glossary term to be used to clearly scope the data in question. Here is a potential, admittedly simple, initial definition to consider:

BES Data – Electronic data used by BES Cyber Systems to perform Supervisory Control and Data Acquisition (SCADA).

The intent of the concept of "demarcation points" is well-reasoned and CHPD supports this identification capability. CHPD requests that the Technical Rationale and Justification (TR&J) for this section be more clearly aligned with the Requirement R1.2, which does not currently limit the scope to the Responsible Entity's Control Center. Consider the following revision:

"1.2 Identification of *the Responsible Entity's* demarcation point(s)…"

A change to a demarcation point in one system should not create a paperwork or compliance issue for a neighbor or vice versa. Alternatively, consider defining the term "demarcation point" in the NERC glossary to identify the scope within the definition of the term, rather than in the language of the standard.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

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

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	

Austin Energy (AE) generally agrees with the Draft 2 revision. However, the SDT should define the new terms “monitoring data” and “control data” in the NERC Glossary. Additionally, the concept of “demarcation point(s)” is unclear. The Standard should indicate a Registered Entity should identify the Cyber Asset at which the Entity begins protected data and ceases to protect data. The current wording implies each entity should document its demarcation point and any demarcation point(s) at a neighboring system. A change to a demarcation point for one entity should not create a paperwork or compliance issue for a neighbor. Alternatively, the SDT could define “demarcation point.”

Also, while the Technical Rationale and Justification for CIP-012 addresses R1 (scope, demarcation points, roles and responsibilities), it does not properly address R2. While physical protections may protect confidentiality between Control Centers owned by the same entity, it does not address non-repudiation and, therefore, integrity as defined by NIST 800-53, Revision 4, page B-6. AE asks the SDT to provide additional rationale and justification regarding how the protections are required “…in a manner that reflects the risks posed to bulk electric system reliability,” as stated on page 12 of FERC Order No. 822.

Likes 0	
Dislikes 0	
Response	

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

N&ST believes the draft Technical Rationale and Justification fails to address the applicability of CIP-012 to the exchange of Real-time Assessment data between a BES Control Center and a third party provider of such data. At the same time, the draft Implementation Guidance document clearly indicates that the SDT believes this scenario would be in scope. If this is in fact true, then both the Technical Rationale and Justification and CIP-012 standard document should include explicit statements to that effect.

Likes 0	
Dislikes 0	
Response	

Don Schmit - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	

Comment
See comments from the MRO NSRF for the ballot conducted for CIP-012-1 which closed on December 11, 2017.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	No
Document Name	

Comment
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-004-011. The obligation can be accomplished with one requirement, as follows. “The Responsible Entity shall implement one or more documented process(es) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring and control data while being transmitted between any Control Centers, except under CIP Exceptional Circumstances. This excludes oral communications. The process(es) shall identify: 1.1 security protection used to mitigate risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. 1.2 demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers. Demarcation points identified by the Responsible Entity do not add additional Cyber Assets to the scope of the CIP Reliability Standards; and 1.3 roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.” This also includes important scoping from the implementation guidance that belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
While the Technical Rationale and Justification for CIP-012 goes into great detail for R1 to give an understanding and overview of the rationale behind the scope, demarcation points, and the need for roles and responsibilities, SRP asserts it did not properly address Requirement 2. While physical protections may satisfy the objective of protecting confidentiality between Control Centers owned by the same Registered Entity, it does not address non-repudiation in any situation, and therefore integrity as it was defined by NIST 800-53, Revision 4, page B-6. SRP requests the SDT

provide more rationale and justification as to how these protections are being required "…in a manner that reflects the risks posed to bulk electric system reliability," as stated on page 12 of FERC Order No. 822.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Support Terry Harbour comments (Berhshire Hathaway Company - MidAmerican Energy Company)

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC ("CenterPoint Energy") does not agree with certain comments in the draft Technical Rationale and Justification. As detailed in its Comment Form for proposed CIP-012-1, CenterPoint Energy recommends that the phrase "and control" be removed from proposed Requirement R1 on page 4 of the draft Technical Rationale and Justification. Inclusion of this phrase may create confusion and does not align with TOP-003 and IRO-010 data specification Requirements. Additionally, the phrase was not mentioned in FERC Order 822. Thus, CenterPoint Energy recommends corresponding revisions to the Technical Rational and Justification.

The SDT's justification on page 5 of the draft Technical Rationale and Justification for adding "and control" to "Real-time monitoring and control data" is unclear and confusing. The SDT recognizes that "in practice Real-time control data is not transmitted separately from Real-time monitoring data." Given this practice, the introduction of the concept of separately transmitted "Real-time control data" may create confusion on whether there are additional data specification responsibilities besides those detailed in TOP-003 and IRO-010.

To align with the revisions recommended above and in its Comment Form for proposed CIP-012-1, CenterPoint Energy also recommends that the following sentences be removed from the first paragraph of page 5 of the draft Technical Rationale and Justification:

"The SDT notes that it expanded the phrase 'Real-time monitoring' from TOP-003 and IRO-010 to 'Real-time monitoring and control' data."

"However, the SDT wanted to ensure that Real-time control data was included regardless of whether or not it is transmitted along with Real-time monitoring data."

CenterPoint Energy believes the rest of the first paragraph on page 5 is appropriate to be included because it states the SDT's thought process and concern.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Under the General Considerations section of the Technical Rationale, Xcel Energy has concerns with implementation of this Standard as related to the term and definition of Control Center. Specifically, we are concerned with the definition of an "associated data center" as part of the Control Center. The Standard does not appear to apply to communication between the control center and a field device (per reference model on page 5 of Technical Rationale). However, if we have a Control Center communicating with a device that aggregates multiple field devices, is that aggregating device location considered an associated data center? Under the Alignment with IRO and TOP Standards, we believe that the types of data to be within scope, as identified by data specification lists originating from TOP-003 and IRO-010 are not specific enough to determine or limit the types of data or communication methods that would need to be protected as Real Time Assessments, Real Time Monitoring, or Control Data. These lists contain data and methods of communicating data that Xcel Energy would not classify as Real Time Assessment, Real Time Monitoring, or Control Data. Xcel Energy's concern is that NERC and Regional Entities may. The inclusion of all data types and methods on these lists could bring systems like corporate email into scope, which we would adamantly oppose. We suggest adding further clarification as to what types of data are included as Real Time Assessment, Real Time Monitoring, and Control Data.	
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	
We support SRP and Chelan PUD comments.	
Likes 0	
Dislikes 0	
Response	

Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	

Tacoma Power endorses the draft comments shared with it by Salt River Project (SRP), which follow:

While the Technical Rationale and Justification for CIP-012 goes into great detail for R1 to give an understanding and overview of the rationale behind the scope, demarcation points, and the need for roles and responsibilities, SRP asserts it did not properly address Requirement 2.

While physical protections may satisfy the objective of protecting confidentiality between Control Centers owned by the same Registered Entity, it does not address non-repudiation in any situation, and therefore integrity as it was defined by NIST 800-53, Revision 4, page B-6. SRP requests the SDT provide more rationale and justification as to how these protections are being required "…in a manner that reflects the risks posed to bulk electric system reliability," as stated on page 12 of FERC Order No. 822.

Likes 0	
Dislikes 0	
Response	

John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	

This is reasonable given that some of the communications may flow on third-party networks. That said, there seems to be no discussion of protecting the communications devices themselves. Recommend taking a "high watermark" approach to categorizing the importance and risk of communication systems. Many utilities use internal communications between their PCC and BCC. If those links are not trusted and require the protections of CIP-012, why trust the substation SCADA links feeding data to the control centers? Being more prescriptive would be helpful. Is the SDT mandating encryption? What physical protections would be sufficient? Is OPGW fiber "protected" or just "difficult?"

Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Page 5 (Control Center Ownership) - Recommend changing ‘ensure adequate protection is applied’ to ‘ensure the security objective is met’ in the sentence, *‘It is strongly recommended, however, that these partnering entities develop agreements, or use existing ones, to define responsibilities to ensure adequate protection is applied.’*

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	Yes
Document Name	

Comment

The California ISO supports the comments of the IRC Security Working Group (SWG)

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

The SPP Standards Review Group proposes to include the defined terms “Confidentiality” and “Integrity” in the NERC Glossary of Terms or, at a minimum, define the terms in the body of the standard. The current definitions are stated in the National Institute of Standards and Technology’s (NIST) Special Publication 800-53A, Revision 4 (as footnoted in the Technical Rationale Documentation); however, the NIST document is non-governing and could be revised outside the purview of NERC, which could have a negative impact on an entity’s compliance with standards such as CIP-012. The SPP Standards Review Group would recommend utilizing the definitions for “Confidentiality” and “Integrity” as stated in the current Technical Rational and Justification for CIP-012.

Additionally, the SPP Standards Review Group would recommend the same course of action be applicable to the term “Demarcation Point.”

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	
Comment	
ERCOT signs onto the comments of the SRC/ITC/SWG of the IRC, pasted below. The SRC & ITC SWG offers the following comments and recommendations. To solidify the intent of the SDT, as noted in the response to comments, the SRC & ITC SWG recommend that it be clarified in the Technical Rationale and Justification that CIP-012-1 is a standalone Standard similar to CIP-014 and is not intended to increase the scope of applicable systems to be protected under CIP-003 thru CIP-011.	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC & SWG - 2 - MRO,NPCC,SERC,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Comments: The SRC & ITC SWG offers the following comments and recommendations. To solidify the intent of the SDT, as noted in the response to comments, the SRC & ITC SWG recommend that it be clarified in the Technical Rationale and Justification that CIP-012-1 is a standalone Standard similar to CIP-014 and is not intended to increase the scope of applicable systems to be protected under CIP-003 thru CIP-011.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eleanor Ewry - Puget Sound Energy, Inc. - 1,3,5	
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	
Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1,3	
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	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Leonard Kula - Independent Electricity System Operator - 2	
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 and ISO-NE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE is concerned about the use of the term “or” as used in Requirement R1. Please see Texas RE's comments for Question #1 on the unofficial comment form for the comment period ending on December 11, 2017.

Texas RE also has a concern about the difference between monitoring and control data. On page 5 of the Technical Rationale, the SDT notes that it expanded the phrase “Real-time monitoring” data from TOP-003 and IRO-010 to “Real-time monitoring and control” data. The SDT was concerned that data transmitted between Control Centers that results in the physical operation of BES Elements was not explicitly included in Real-time monitoring data. The SDT understands that in practice Real-time control data is not transmitted separately from Real-time monitoring data. However, the SDT wanted to ensure that Real-time control data was included regardless of whether or not it is transmitted along with Real-time monitoring data. If entities only transmit Real-time control data along with Real-time monitoring data, then the SDT does not intend for such entities to identify additional data beyond that Real-time monitoring data already included in the data specifications for TOP-003 and IRO-010. Texas RE is concerned that if there is a need to expand the phrase to include control data in CIP-012-1, there might also be a need in IRO-010 and TOP-003.

Likes 0	
Dislikes 0	

Response

2. The SDT developed draft Implementation Guidance for CIP-012 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.

Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	

Comment

Tacoma Power endorses the draft comments shared with it by Salt River Project (SRP), which follow:

The Implementation Guidance states "The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers for the entire distance between CIP-012-1 demarcation points." The document also describes a situation where Entity Alpha exchanges data with Entity Beta through a "3rd party network." The guidance asserts "a number of security controls may be leveraged such as network segmentation and system access control to protect the data as it transits the 3rd party network." However, the document does not describe the implications if the third part circumvents these controls. Additionally, these controls within the 3rd party network do not address non-repudiation, and therefore integrity as it was defined by NIST 800-53, Revision 4, page B-6. SRP asserts more explanation is required within the Implementation Guidance to explain how the example approaches satisfy the security objective. If the approaches indeed satisfy the security objective, then the requirement must be updated to fit the scenario.

Although the SDT states it does not specify controls, the only examples provided in the implementation guidance includes encryption. If there are other methods available other than encryption to achieve the security objective, please provide them.

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

We support SRP and Chelan PUD comments.

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	
Comment	

For the same reasons discussed in its Response to Question No. 1 and in its Comment Form for proposed CIP-012-1, CenterPoint Energy recommends that the phrase “and control” be removed from Requirement R1on page 4 of the draft Implementation Guidance..

In accordance with Requirement R1.3, Responsible Entities are required to identify roles and responsibilities for applying security protections. However, on page 5 of the Implementation Guidance, consideration of the following situations was listed: (1) configuration of security protocols, (2) responding to communication failures, and (3) responding to Cyber Security Incidents. Items (2) and (3) go beyond the scope of Requirement R1.3 and, therefore, should be removed from the Implementation Guidance.

Similarly, on page 9, the following example goes beyond the scope of Requirement 1.3 and should be removed from the Implementation Guidance:

“Entity Alpha and Entity Beta have agreed to a 30 character pre-shared key for coordinated response to any communication failures. They have also exchanged contact information for their Security Operations Centers to enable a coordinated response to any suspected Cyber Security Incidents.”

Page 8 and page 13 lists “AES-128 encryption” as an example of protection; however, 128 bit encryption is the lowest key length. CenterPoint Energy recommends removing “AES-128” and only stating the word “encryption.”

In the last paragraph of page 9, regarding communications through a third party, the Implementation Guidance should recommend stronger controls around protecting the data being transmitted through a third party communication link. For example, Entity Alpha and Entity Beta should establish agreements with the 3rd party responsible for the communication to protect the data transiting its network. The last sentence, “The 3rd party may take responsibility for protecting the data transiting its network” does not allow for adequate protection of the data.

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

Support Terry Harbour comments (Berhshire Hathaway Company - MidAmerican Energy Company)

Likes 0	
Dislikes 0	
Response	

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

Answer	No

Document Name	

Comment

The Implementation Guidance states “The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers for the entire distance between CIP-012-1 demarcation points.” The document also describes a situation where Entity Alpha exchanges data with Entity Beta through a “3rd party network.” The guidance asserts “a number of security controls may be leveraged such as network segmentation and system access control to protect the data as it transits the 3rd party network.” However, the document does not describe the implications if the third part circumvents these controls. Additionally, these controls within the 3rd party network do not address non-repudiation, and therefore integrity as it was defined by NIST 800-53, Revision 4, page B-6. SRP asserts more explanation is required within the Implementation Guidance to explain how the example approaches satisfy the security objective. If the approaches indeed satisfy the security objective, then the requirement must be updated to fit the scenario.

Although the SDT states it does not specify controls, the only examples provided in the implementation guidance includes encryption. If there are other methods available other than encryption to achieve the security objective, please provide them.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	No
Document Name	

Comment

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-004-011. The obligation can be accomplished with one requirement, as follows. “The Responsible Entity shall implement one or more documented process(es) to mitigate the risk of the unauthorized disclosure or modification of Real-time Assessments and Real-time monitoring and control data while being transmitted between any Control Centers, except under CIP Exceptional Circumstances. This excludes oral communications. The process(es) shall identify: 1.1 security protection used to mitigate risk of unauthorized disclosure or modification of Real-time Assessment and Real-time monitoring and control data while being transmitted between Control Centers. 1.2 demarcation point(s) where security protection is applied for transmitting Real-time Assessment and Real-time monitoring and control data between Control Centers. Demarcation points identified by the Responsible Entity do not add additional Cyber Assets to the scope of the CIP Reliability Standards; and 1.3 roles and responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring and control data between Control Centers, when the Control Centers are owned or operated by different Responsible Entities.” This also includes important scoping from the implementation guidance that belongs in the requirement, that demarcation points don’t add additional Cyber Assets to the scope of the CIP standards. Also, the Proposed Reliability Standard lacks sufficient specificity (i.e., sufficient to stand on its own), without an endorsed Technical Rationale and Implementation Guidance. Relative to the draft Implementation Guidance document, MEC agrees with EEI that Industry will likely find it difficult to make any final judgments on the proposed Reliability Standard without NERC's endorsement of the draft Implementation Guidance. We trust that once the Proposed Reliability Standard gets closer to a final ballot NERC will endorse the final draft of the Implementation Guidance. In the event that doesn't occur, we fear the approval of this standard may be at risk.

Likes 0	
Dislikes 0	

Response

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

N&ST believes that Figure 4 (“Network Diagram depicting communications through a 3rd party”) and its accompanying discussion describe a scenario for which CIP-012, as presently written, would not apply. As the figure is presently drawn, Control Centers “Alpha” and “Beta” are not communicating, that is, exchanging data, with each other. Each one is communicating with the “3rd party.” The fact that the 3rd party is presumably forwarding data t*hat it has processed in some fashion* to Beta after receiving it from Alpha, or vice-versa, does not, in N&ST’s opinion, constitute communications *between* two BES Control Centers.

If the SDT believes that communication links carrying Real-time Assessment data between BES Control Centers and 3rd party providers of such data, then CIP-012-1 should be modified to make this an explicit requirement.

Likes 0	
Dislikes 0	
Response	

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	

AE requests a formal definition of terms describing the data in question (*e.g.* “BES data” to address “monitoring” and “control” data types in a single definition. BES Data could be defined as, “Electronic data in BES Cyber Systems used to perform Supervisory Control and Data Acquisition (SCADA).” If the STD believes monitoring and control data should be defined separately, AE requests new NERC Glossary terms for “monitoring data” and “control data.”

Additionally, the Implementation Guidance states “The protection must also meet the security objective of mitigating the risk of unauthorized disclosure or modification of applicable data while in transit between Control Centers for the entire distance between CIP-012-1 demarcation points.” The document describes a situation where Entity Alpha exchanges data with Entity Beta through a “3rd party network.” The guidance asserts “a number of security controls may be leveraged such as network segmentation and system access control to protect the data as it transits the 3rd party network.” The document does not, however, describe the implications of the 3rd party circumventing those controls. Additionally, the controls in the 3rd party network do not address non-repudiation and, therefore, integrity as defined in NIST 800-53, Revision 4, page B-6. AE requests additional explanation to explain how the example approaches meet the security objective.

Although the SDT states it does not specify controls, the only examples provided include encryption. If other methods exist, the SDT should provide them.

Likes 0	

Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 1,3,5,6, Group Name Chelan PUD	
Answer	No
Document Name	

Comment
The Technical Rationale and Justification (TR&J) does not currently provide any technical implementation guidelines to identify where protections may be applied under the language of the CIP-012-1 standard. CHPD requests the addition of one or more sample connectivity drawings to the TR&J that depict compliant topology configurations showing the R1.1 security protection and R1.2 demarcation point placement that could be applied to an existing pair of in-scope Control Centers, including the associated BCS, ESP (EAP/EACMS), and PSP boundaries.

Likes 0	
Dislikes 0	

Response

David Francis - SRC & SWG - 2 - MRO,NPCC,SERC,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	

Comment
Comments: There are concerns regarding the statement, “Demarcation points identified by the Responsible Entity do not add additional assets to the scope of the CIP Reliability Standards.” Entities may already include the demarcation points as Cyber Asset relevant to CIP-002 thru CIP-011. The statement could be revised as, “Demarcation points identified by the Responsible Entity is not intended to add additional assets to the scope of the CIP Reliability Standards.” With regards to the references models and narrative, it would be helpful to have the narrative and the reference model together. It is cumbersome to keep skipping back and forth in the document.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment
Comments: There are concerns regarding the statement, “Demarcation points identified by the Responsible Entity do not add additional assets to the scope of the CIP Reliability Standards.” Entities may already include the demarcation points as Cyber Asset relevant to CIP-002 thru CIP-011. The statement could be revised as, “Demarcation points identified by the Responsible Entity are not intended to add additional assets to the scope of the CIP Reliability Standards.” With regards to the references models and narrative, it would be helpful to have the narrative and the reference model together. It is cumbersome to keep skipping back and forth in the document.

Likes 0	
Dislikes 0	

Response

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	

Comment
While PNMR agrees with the example approaches in the draft Implementation Guidance there is one scenario that does not appear and possible should. Some entities use mailbox or virtual RTUs to communicate data between Control Centers either as redundant method to or in lieu of ICCP. Some Entities may forget that such communication could be in-scope of the standard especially if “Real-time Assessment and Real-time monitoring and control data” is passed through these mailbox or virtual RTUs. Typically these have points to point serial protocols and those serial connections would need to have protections applied. While PNMR does not know how many still use mailbox or virtual RTUs as an alternate means, it is something the drafting team should take into consideration.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	

Comment
Xcel Energy agrees that the approaches offered in the CIP-012-2 Implementation Guidance are non-prescriptive and can be sufficient models to be used in implementation. However, Xcel Energy cannot agree with the proposed timeline of 24 months. We share real-time data with Registered Entities (REs) such as the Reliability Coordinators (RCs) including MISO, SPP and PEAK. Additionally, we would share data with many utilities with Control Centers across our service territory. Finding a common technological solution to implement the proposed mitigating activities in the

Requirements will take a substantial effort on the part of all REs. Once a common technology and all legal agreements between REs are in place, Xcel Energy may still have to purchase and implement those technology solutions.

Xcel Energy stakeholders suggest that NERC should advice and work with all RCs to agree upon a common technology first and then drive those solutions from the RC down to each utility in scope.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Exelon generally agrees with the approach in the draft Implementation Guidance, noting the following concerns and suggestions.

1. We have a concern that the CIP-012-1 Standard may be approved prior to NERC endorsement of the Technical Rationale and Justification and the Implementation Guidance for CIP-012. Our approval of the CIP-012-1 Standard language as presented is in part predicated upon the clarifications present within the Implementation Guidance. We would expect to see the endorsement by NERC of these supporting documents before we vote for final approval of the Standard.

2. Within the Standard, Technical Rationale and Justification, and the Implementation Guidance, there is no mention of the scenario of data transmission between a Control Center and its associated Data Center(s) located in separate physical locations. Clarification of whether this intra-Control Center data transmission is in scope seems appropriate.

3. Our SMEs raised questions about data not currently determined to have a 15-minute impact and therefore out of scope for CIP-002 thru CIP-011, e.g. synchrophasers data. Can we automatically assume then, that this same data is also currently out of scope for CIP-012? Looking for clarification on this question within the Standard or supporting documents.

Likes 0	
Dislikes 0	

Response

Eleanor Ewry - Puget Sound Energy, Inc. - 1,3,5

Answer	Yes
Document Name	

Comment

Further details about the technological controls required to meet the requirements would be helpful. Providing additional, specific examples about appropriate approaches would help ensure entities implement sufficient protection mechanisms, per the requirements.

Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The California ISO supports the comments of the IRC Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Page 1 Introduction - Recommend including in the Introduction the same paragraph found in the Technical Rationale and Justification Introduction as it provides an important perspective that appears to not be fully understood. *'Although the Commission directed NERC to develop modifications to CIP-006, the SDT determined that modifications to CIP-006 would not be appropriate. There are differences between the plan(s) required to be developed and implemented for CIP-012-1 and the protection required in CIP-006-6 Requirement R1 Part 1.10. CIP-012-1 Requirements R1 and R2 protect the applicable data during transmission between two separate Control Centers. CIP-006 Requirement R1 Part 1.10 protects nonprogrammable communication components within an Electronic Security Perimeter (ESP) but outside of a Physical Security Perimeter (PSP). The transmission of applicable data between Control Centers takes place outside of an ESP. Therefore, the protection contained in CIP-006-6 Requirement R1 Part 1.10 does not apply.*'	
Likes 0	
Dislikes 0	
Response	
John Tolo - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	

Comment
Sometimes the lack of specifics causes confusion and lost time. Being more specific about the technological controls would be more helpful. For instance, PCI-DSS specifically calls out when encryption is needed for data at-rest and in-transit. If the intent is to encrypt data, it would be better to say so up-front and specify the protection boundaries. Some entities may decide to implement different protection mechanisms that may not be sufficient from a security perspective and then through the course of presentations and guidance have to re-work. TEP appreciates the opportunity to comment.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - FRCC,MRO,WECC,Texas RE,SERC,SPP RE	
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 and ISO-NE	
Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
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	
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	
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	

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE has the following comments regarding the implementation guidance:

In the Identification of Security Protection section on page 6: "*Alternatively, a Responsible Entity* may *demonstrate implementation through* ***monitoring*** *of the security control such as a report generated from an automated tool that* ***monitors*** *the encryption service used to protect a communications link*."

- Texas RE recommends adding monitoring **and logging**, monitors **and logs**.

In the Reference Model Discussion for Requirement R1 section on page 7:

"*Additionally, Entity Alpha does not need to consider any communications to other non-Control Center facilities such as generating plants or substations. These communications are out of scope for CIP-012-1*."

- Although this may be out-of-scope as a best security practice, Texas RE recommend Entity Alpha should "*consider any communications to other non-Control Center facilities such as generating plants or substations*."

In the Identification of Security Protection section on page 13:

"*When physical security controls are used, Entity Alpha* ***may*** *demonstrate the implementation of physical protection* ***using a floorplan diagram*** *showing the physical access controls in place*."

- Texas RE suggests including other types of evidence with a floorplan as a floorplan diagram alone would not be sufficient.

Likes 0	
Dislikes 0	
Response	