Comment Report

Project Name:	2016-02 Modifications to CIP Standards | Communication Networks
Comment Period Start Date:	2/10/2017
Comment Period End Date:	3/13/2017
Associated Ballots:	

There were 48 sets of responses, including comments from approximately 121 different people from approximately 91 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time. Do you agree with the SDT's assertion? If you agree, please supply a rationale to support the position.

2. If you do not agree with the SDT's assertion in Question 1, please identify the type of data, the risk posed at rest, and supply the rationale to support the position.

3. Future enforceable Reliability Standards IRO-010-2 and TOP-003-3 identify "data required for reliable operation." For example, Requirement R1 of IRO-010-2 states:

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Realtime Assessments including non-BES data

TOP-003-3 Requirements R1 & R2 also have similar requirements for BAs and TOPs.

Do you agree that outlining this approach for identifying "data required for reliable operation" in the Guidelines and Technical Basis is sufficient; consequently, an additional definition of "sensitive BES data" or a requirement to identify "sensitive BES data" is not necessary? If not, please explain.

4. The SDT asserts that "availability" of inter-and intra-entity Control Center communication of data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards, specifically Reliability Standards TOP-001-4 and IRO-002-5. The proposed standards require redundant and diversely routed data exchange capabilities at a Responsible Entity's primary Control Center. Do you agree that "availability" is adequately addressed by these standards? If not, please provide rationale to support your position.

5. The SDT is proposing to develop a new CIP standard because the directives of FERC Order 822 related to the protection of communication networks used to exchange sensitive BES data regardless of the entity's size or impact level. Do you agree with the drafting of a new CIP standard to address this issue? If you disagree and would prefer to include requirements in existing CIP Standards, such as CIP-003 and CIP-005, please provide rationale and propose requirement language.

6. The SDT evaluated multiple approaches to addressing the directive. The approach proposed in this informal posting focuses on the protection of communication links. An alternative approach could focus on the protection of the sensitive BES data itself. Do you agree with the SDT's approach to focus the draft language on the protection of communication links? If not, please provide rationale and propose alternative language.

7. Do you agree with the security objective of the draft language? If not, please propose alternative language.

8. Is it clear what types of plans, procedures, and methods are needed to meet the draft language? If not, please propose alternative language.

9. The SDT uses the term "communication networks" throughout the draft language including an obligation to define the boundaries of such communication networks. Does the SDT need to define the term for inclusion in the NERC Glossary of Terms? If so, please propose a definition of "communication networks."

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC

Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3,4,5		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
Con Ed - Consolidated Edison Co. of New York	Kelly Silver	1,3,5,6	NPCC	Con Edison	Kelly Silver	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange and Rockland Utilities	NA - Not Applicable	NPCC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC

					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO

					Chuck Lawrence	American Transmission Company	1	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Mike Buyce	City Utilities of Springfield	1,4	SPP RE
					Robert Gray	Board of Public Utilities,KS (BPU)	3	SPP RE
					Stewart Dover	Lafayette Utilities System	2	SPP RE

					John Allen	City Utilities of Springfield, Missouri	4	SPP RE
Public Service Enterprise Group	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 asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time. Do you agree with the SDT's assertion? If you agree, please supply a rationale to support the position.

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE requests the SDT consider defining the term "sensitive BES data", which could include ICCP, Historian, and backup data, since a goal of this project should be to provide clear requirements for identifying and protecting Control Centers required for reliable operation. The undefined term, sensitive BES data, is already being used among several non-CIP standards and defining the term would encourage consistency and lessen confusion.	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP contends that CIP standards, specifically CIP-003,005,006, 007, 009, 010, and 011 concentrate on BCS, EACMS, PCA, PACS devices and data resident on them.	
Likes 0	
Dislikes 0	
Response	

Gerry Adamski - Essential Power, LLC - 5	
Answer	No
Document Name	
Comment	

Is the operational data a subset of all sensitive data? I would offer that certain modeling update information would not fall under this framework and could have negative impacts on the BES (e.g. ratings changes, configuration/outage changes, etc.). If that is captured in the scope of operational data, then ok but I infer from the presentation of the information that real-time variable data is what is being targeted here.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Reclamation recommends removing the phrase “is perishable, and has a diminished need for protection over time.” Reclamation agrees that data at rest is already afforded protections under other applicable CIP standards. Reclamation disagrees that all data at rest is perishable and has a diminished need for protection over time.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS agrees with the assumption that data at rest within a Control Center is already afforded protections under existing CIP standards (CIP-003-6, CIP-005-5, CIP-007-6, etc.), but respectfully notes that this assumption is outside the scope of the directive set forth by FERC in Order No. 822. Pursuant to FERC Order No. 822, Paragraph 53, the directive targets communication links and data **communicated between bulk electric system (“BES”) Control Centers.** (Emphasis Added.) Thus, the directive does not encompass or extend to include data at rest within BES Control Centers. Rather, it is intended to ensure that data in transit between such Control Centers are afforded appropriate protections. To ensure that the scope of the directive is accurately captured, AZPS offers the following revision to the referenced assumption:

Data at rest within a BES Cyber System is already afforded protections under existing CIP standards and is not within the scope of this directive.

Likes 0	

Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Currently many PI or other Historians that store near real time data are located outside of ESPs since this data, once it is stored on the Historian is not used for operations. ***However some entities may use data stored on Histroians as a feedback loop into their control systems***. In these specific siturations the data "at rest" on the Historians may have an operational impact. Data that resides within an entities EMS is constantly being updated, the "data points" exist in memory and store data values in these data points are constantly being updated. If data wishes to be preserved it is written to a histroian before being overwirtten.	
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	

Data needed for the operation of the BES is already protected and exists only to transmit operational controls which are transient in nature.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

The NSRF agrees with the SDT. NERC has already defined Operating Reliability Data (ORD) and recipients are required to sign an ORD Confidentiality Agreement, which should elimate the need for a requirement. Additionally, NERC Standards of Conduct as well as most FERC approved tariffs have provisions for protection of sensitive data.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

SRP agrees with the SDT assertions:

- CIP-003: Identifies all security management controls used by the entity to address high, medium, and low impact BES Cyber Systems (BCS).
- CIP-004: R4 Part 4.1 requires entities to develop processes to control not only electronic and physical access, it also requires processes to control access to designated BES Cyber System Information storage, otherwise known as repositories, as determined in CIP-011. These repositories are where “referenced data” would exist “at rest”.
- CIP-005: The entirety of the Standard is based on specifying a controlled Electronic Security Perimeter (ESP) in supporting of protecting BCS (including information “at rest” within the BCS).

- CIP-006: In the same manner as CIP-005 and ESP protections, the physical protections afforded by CIP-006 protect the BCS from unauthorized individuals “walking-up” to components of the BCS where “at rest” “referenced data” may exist.
- CIP-007: The entirety of the Standard is based on specifying technical, operational, and procedural controls to protect the BCS (including the information “at rest” within the BCS).
- CIP-010: The change and configuration management controls prevent and detect unauthorized changes to the BCS (including information “at rest” within the BCS). Vulnerability assessment requirements are also in support of protecting the BCS (including information “at rest” within the BCS).
- CIP-011: R1 requires the identification of BES Cyber System Information. An article of acceptable evidence included in the measures of R1 is the identification of “repositories or electronic and physical locations designated for housing BES Cyber System Information”. These identified locations are used as input for CIP-004 R4 Part 4.1 (in order to verify access controls).

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

The same information that is two seconds old in a real-time SCADA system may be retained for five years in a corporate (non-control) data historian. NERC CIP-002-5.1 scopes the applicability of the protections on assets which have a real-time impact on reliable BES operations. As such, any information utilized by real-time systems for a fifteen minute time horizon are already afforded protections in CIP-002 through 011.

While data at rest may have impacts on planning or historical analysis, it cannot be reasonably inferred to have a fifteen minute impact on reliable operations. Many multi-purpose Operating Systems support encrypted file systems. As such, any mandate for data at rest protections would be more appropriately scoped in CIP-011 and applied to electronic repositories of BES Cyber System information.

The Confidentiality, Integrity and Availability triad is commonly utilized in designing effective controls for information systems. Regulatory frameworks which provide protections for data at rest are focused on confidentiality of financial transactions and/or Personally Identifiable Information. Power control systems have unique characteristics which make Availability and Integrity paramount.

Encryption for data at rest inherently is focused on making access to information more restricted. This inherently creates potential to adversely impact Availability, which may be counter-productive to reliable BES operations.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
We agree that existing CIP standards protections address the referenced data at rest. The referenced data is covered in the cited Standards. Consider that real-time SCADA data performance may be impacted by disk encryption.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the assertion that the referenced data is already afforded protections under existing CIP standards.	
Likes 0	

Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
The data is resting on systems that are protected by CIP controls.	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
NRG agrees with the rationale because, the data at rest is not being used in the real-time operation of the Bulk Electric System i.e. the 15 minute impact process. Also, the CIP Standards provide the appropriate protection for data integrity and confidentiality for in-scope systems.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

The referenced data while at rest is covered in the cited Standards. Consider that real-time SCADA data performance may be impacted by disk encryption.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Once referenced data has been received by a BES Cyber Asset it is then protected under the CIP Standards. There is no need to protect stale data.	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Once referenced data has been received by a BES Cyber Asset it is then protected under the CIP Standards. There is no need to protect stale data.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment	
ERCOT agrees with the SDT's assertion. ***While at rest***, the data required for reliable operation resides within existing BCS data and is afforded protections under existing CIP Standards. Much of the referenced data has a limited time of need for protection and can be made public after a certain number of days. Requiring additional protections of data at rest may not be necessary and due to the limited time of sensitivity, may not have a positive cost benefit.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
In use and transport is the highest risk. Exisiting controls are sufficient.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA agrees with the SDT assertion. BPA believes the referenced data is already afforded protections at rest under existing standards.	
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 with the rationale that the data is perishable and is already afforded protection under existing CIP standards. Any data that is at rest does not meet the 15-minute impact criteria for adversely impacting real-time operations.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Existing CIP-011 requirements adequately identify and protect BES Cyber System information at rest.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Access to the host systems is strictly controlled via the current CIP standards and requirements.	
Likes 0	

Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Basin Electric Power Cooperative agrees NERC has already defined Operating Reliability Data and recipients are required to sign a Confidentiality Agreement, which should elimate the need for a requirement. In addition, Basin Electric agrees existing CIP standards provide protection for this data at rest.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Yes, Southern Company agrees with the SDT's assertion. Real-time reliability data used by Control Centers is only sensitive within a short time window; it becomes perishable quickly and the need to maintain protections for that data diminishes over time. For data "at rest", Southern Company views the language in the FERC Order, specifically paragraph 54, intending to address a reliability gap to protect communications between Controls Centers from "data manipulation type attacks" and "eavesdropping attacks". The existing controls applied in accordance with CIP-011 and CIP-006-6 R1.10 sufficiently address protection of sensitive BES data "at rest" and in logical transit within an ESP, respectively. Additionally, the existing controls applied in accordance with CIP-004 (Access Management), CIP-005 (ESPs, encryption, multi-factor authentication), and CIP-007 (system security controls, account management) provide by extension added layers of security to protect data "at rest."	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes

Document Name	COMM Network - Exelon Comments - 3.13.17.docx
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
AECI agrees that the referenced data is already afforded protections at rest under the current CIP Standards. Operational Reliability Data becomes stale over time and has a diminished need for protection.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
The referenced data is covered in the cited Standards. Consider that real-time SCADA data performance may be impacted by disk encryption.	
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 agrees with the rationale because, the data at rest is not being used in the Real-time operation of the Bulk Electric System i.e. the 15 minute impact process. Also, the CIP Standards provide the appropriate protection for data integrity and confidentiality for in scope systems.	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Yes, much of the critical data between control centers is only valid for that immediate time period, control data hours or days old only has historical value.	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	Yes
Document Name	
Comment	
• NERC has already defined Operating Reliability Data (ORD). Additionally, recipients are required to sign an ORD Confidentiality Agreement, which should elimate the need for a requirement.	
Likes 0	
Dislikes 0	

Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
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	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
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	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	

Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 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	

2. If you do not agree with the SDT's assertion in Question 1, please identify the type of data, the risk posed at rest, and supply the rationale to support the position.

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

Answer	
Document Name	

Comment

No comment

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	
Document Name	

Comment

AZPS respectfully asserts that the SDT's assertion in Question 1 is beyond the scope of the directive set forth in Order 822 at paragraph 53. Further, AZPS is concerned that the assumption paints all data retained with BES Control Centers with too "broad of a brush stroke." This is particularly evident in the SDT's assumption that all data within Control Centers is perishable and has a diminished need for protection as such statements appear to be considering the "freshness" of real-time data only.

AZPS notes that the data contained and retained within BES Control Centers includes more than real-time data. In particular, BES Control Centers often also retain data related to the operations and long-term planning time horizons. Such data, which is outside of data indicative of real-time status, may not age and become perishable in the same manner or time period as data communicating real-time status. Because the verbiage utilized in the assumption is extremely broad and does not clearly distinguish the or otherwise narrow the specific data to which the assumption applies, AZPS disagrees with the assumption set forth by the SDT as such assumption has the effect of "broad brushing" all data communicated between and "at rest" within BES Control Centers with the same importance and usability when, in fact, such data has varying levels of criticality, usability, confidentiality, etc.

AZPS reiterates that it agrees with the SDT that the risk associated with data "at rest" within Control Centers is negligible given the applicability of existing CIP reliability standards to such data, but, for the reasons set forth above, must respectfully disagree with the assumption and re-urge the SDT to adopt the proposed revisions recommended in response to Question 1.

Likes 0	
Dislikes 0	

Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	
Document Name	
Comment	
Not Applicable	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	
Document Name	
Comment	
n/a	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	
Document Name	
Comment	
N/A	
Likes 0	

Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Reclamation recommends removing the phrase “is perishable, and has a diminished need for protection over time.” Reclamation agrees that data at rest is already afforded protections under other applicable CIP standards. Reclamation disagrees that data all at rest is perishable and has a diminished need for protection over time. Reclamation recommends that each entity be responsible to determine the value of its data at rest, if and when the data at rest is perishable, and the necessary level of protection. As examples, some data between control centers may include sensitive data such as configuration information of the network or relay protection systems. If the data that is transferred is deemed to be sensitive, then the associated data at rest may also be sensitive.	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	
Document Name	

Comment	
The CIP standards do not necessarily apply to Cyber Assets that perform operating day ahead activities or other comparable functions that may be capable of impacting the BES beyond the 15 minute threshold.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	
Document Name	
Comment	
N/A	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	
Document Name	
Comment	
HQT’s understanding of the objectives behind the drafting of CIP-012 is to protect communication links and therefore sensitive bulk electric system data exchanged between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posed to the BES by the assets being protected (i.e., high, medium, or low impact). Why are the security objectives are silent regarding avaibility? Protection of data at rest is (currently) not part of the objectives of CIP-012. Furthermore, our understanding of the different CIPs is that it does not fully address the security objectives of confidentiality and integrity of data at rest. CIP-005 is about establishing enclaves to protect the cybet assets, CIP-007 about the protection of the Cybe assets, CIP-011 to prevent unauthorized access (Guidelines and Technical Basis mention confidentiality but not integrity).	

Furthermore, the princips of CIA (Confidentiality Integrity Avaibility) may be implied but they are not precise enough to ensure that the objectives are meet in the existing CIP standards (CIP-003, 005, 007, 011 etc.). The concepts of confidentiality are treated in a certain ways but the concepts of integrity are not explicit. The objectifs of CIP-012 could say ”Develop a security plan to ensure the confidentiality, integrity of data at rest and in-transit between Control Centers, both inter-entity and intra-entity”	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	
Document Name	
Comment	
See above	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	

Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s response to #1.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
See comment above.	
Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
n/a	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
See comments for Question No. 1	
Likes 0	
Dislikes 0	

Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP agrees with the SDT’s assertion in Question 1.	
Likes 0	
Dislikes 0	
Response	

3. Future enforceable Reliability Standards IRO-010-2 and TOP-003-3 identify "data required for reliable operation." For example, Requirement R1 of IRO-010-2 states:

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real -time monitoring, and

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real time monitoring, and Realtime Assessments including non -BES dat

TOP-003-3 Requirements R1 & R2 also have similar requirements for BAs and TOPs.

Do you agree that outlining this approach for identifying "data required for reliable operation" in the Guidelines and Technical Basis is sufficient; consequently, an additional definition of "sensitive BES data" or a requirement to identify "sensitive BES data" is not necessary? If not, please explain.

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
The SDT should refine references to make it clear IRO-010 and TOP-003 data is limited to only data transmitted between control centers, because data between field assets and the control center is not in-scope. Also, this should not be in the Guidelines and Technical Basis section of a Standard because it would not be enforceable.	
Likes 0	
Dislikes 0	
Response	

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes the "data required for reliable operation" identified in TOP-003-3 and IRO-010-2 is too broad and goes beyond the scope of "sensitive bulk electric system data" that should be protected. For example, portions of the data requested in TOP-003-3 and IRO-010-2 could be non-BES data that may only serve a purpose under certain system configurations or conditions. Data specified as necessary for Operational Planning Analyses is based in large part on projections and forecasts which should not fall under the label of "sensitive bulk electric system data." For example, outages, Facility Ratings, equipment limitations, and Protection System degradation use data exchange capabilities (phone systems, email, web based	

portals, FTP exchange, RTU, etc.) which may go beyond 'communication links' between Control Centers and should remain flexible enough to allow for normal and abnormal Real-time system conditions and what Operating Plans are being implemented at that time.

CenterPoint Energy recommends that the drafting team narrow the scope to a subset of the data identified in TOP-003-3 and IRO-010-2. CenterPoint Energy also recommends the drafting team develop criteria in the requirement language for determining what "sensitive bulk electric system data" should be separate from the holistic list of data necessary for functions described in the latest revisions of TOP and IRO Standards. CenterPoint Energy does not believe referencing the TOP-003-3 and IRO-010-2 standards in the requirement language is necessary as this may become problematic in the future if the language in these standards changes or becomes obsolete.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Duke Energy does not agree that a definition of "sensitive BES data" is not necessary. The question above alludes to expectations for the RC/BA/TOP in IRO-010-2 and TOP-003-3, but the reference fails to point out how this would apply to other functions such as the GOP. It is not enough to refer to the RC/BA/TOP data requirements if the standard is also applicable to other functions unless the applicability of data required from the GO/GOP/TO/DP by the RC/BA/TOP is limited.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

SRP agrees that IRO-010-2 is the correct standard to identify "sensitive BES data"; however, SRP believes R3 should be used to determine what an entity is actually sending to the RC, as opposed to R1 (what the RC is asking for). This benefits entities with fewer functional registrations by eliminating data sources that are not applicable to them.

SRP agrees that TOP-003-3 R1 and R2 can be used to identify "sensitive BES data".

TOP-003-3: SRP provides the same evidence for both R1 and R2:

- R1: Data necessary for Operational Planning, Real-time monitoring, and Real-time Assessments.
- R2: Data necessary for analysis functions and Real-time monitoring.

SRP would like to see examples that include sensitive BES data transmitted between primary and back-up Control Centers. SRP also requests clarification on requirements for entities that own their communications network and protection of data transferred within the same private network.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 3,5

Answer	No
Document Name	

Comment

The data for Operational Planning Analysis does not address the data that is used to perform other required functions such as calculating ACE for a BA. Data Required for reliable operation should include Data used during the performance of any Reliability Related Task (RRT) as defined with the entities training program under requirement PER-005-2 R1.1

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NRG suggests that the drafting team develop a definition for the term “sensitive BES data” - something similar in effect to the term “BES Cyber Systems Information” defined for CIP-011. Also, NRG recommends the definition for the term “sensitive BES data” include language addressing the 15 minute impact operational criteria.

NRG’s proposed language for “sensitive BES data” definition: “Data if rendered unavailable, degraded, or misused within 15 minutes would adversely impact the Real-Time operation of the Bulk Electric System.”

Our interpretation of the proposed language is that the drafting team has a concern for the protection of the data being transmitted. Since the data being transmitted can't be broken down and identified as sensitive data or non-sensitive data, the recommendation of developing a definition seems to be the safest path. Additionally, NRG recommends that the drafting team review the term "reliable operation" in the NERC Glossary of Terms. Also, if the term is used in the Requirement, NRG recommends using the term's definition out of the glossary. This is a defined term and we propose that the term should be capitalized. NRG seeks to understand, with this being a defined term, does this change the drafting team's intent for the use of this term?	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
TOP-03-3 R1.1 requires a list of data and information needed, including non-BES data and external network data deemed necessary by the Transmission Operator. Because the requirement is vague using the verbiage such as "information needed" and "non-BES data" it may be difficult or impractical to protect the various methods used to communicate information or non-BES data. Methods of communication could include voice, email, text messages, or faxes.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Responsible Entities are audited to the requirement language and cannot be held to the language in the GTB. If there is a desired outcome from a requirement, it should be stated in the requirement language; the GTB should not be used to imply the inherent meaning of a requirement. If the SDT's intent is to rely on documentation developed in TOP-003, the requirement should state that. If the SDT's intent is to rely on "a list of data and information needed by the Reliability Coordinator to support Operational Planning Analyses," etc., the requirement should state that. The GTB should provide only additional guidance.	
Likes 0	

Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes trying to connect multiple requirements to dissimiliar standards or standard families poses a huge risk in that altering the “origin” standard requirement without also modifying the “destination” requirement may result in a violation.Written guidelines provided by NERC explaining what “sesntive BES data” means would be helpful since the terms can be interpreted in various ways by each RC, BA and TOP.	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
TOP-03-3 R1.1 requires a list of data and information needed, including non-BES data and external network data deemed necessary by the Transmission Operator. Because the requirement is vague using the verbiage such as “information needed” and “non-BES data” it may be difficult or impractical to protect the various methods used to communicate information or non-BES data. Methods of communication could include voice, email, text messages, or faxes.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	

Comment
ERCOT does not agree with the approach of putting this in the Guidelines and Technical Basis section of a Standard since it is not enforceable or recognized by some ERO compliance staff. While the scoping of IRO-010 and TOP-003 may be too broad, having clear criteria will assist in clear implementation and understanding among the entities required to comply with the requirement. Without clear scope being defined, it could be left up to each responsile entity to determine what they think meets this criteria. That seems to be problematic since the responsible entities on each end of the communication link may not agree. It will also cause consistency issues with responsible entities that are under different regions. There will be a constant comparison of practices and could result in auditors determining what is necessary. The SDT should consider refining references to make it clear that IRO-010 and TOP-003 data is limited to only data transmitted between control centers. The data between field assets and the control center is out of scope. Also consider clarifying language that is clear that IRO-010 and TOP-003 informaton that is transferred verbally, including any VoIP, is not included in scope. In lieu of using IRO-010 and TOP-003, the SDT could consider creating a definition of the relevant data. Either of these approaches would be beneficial to facilitate getting necessary understanding, agreements, and/or regional rules implemented. Not having clear criteria will only increase the time needed to implement the standard. Entities will have to negotiate agreement on relevant data and then proceed with implementing protections.

Likes 0	
Dislikes 0	

Response

Gerry Adamski - Essential Power, LLC - 5	
Answer	No
Document Name	

Comment
If it inlcudes system configuration and modeling data that can be modified via inter-entity communication networks, then yes.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	
Comment	

Many of the systems that are identified in the lists required by TOP-003 R1 and IRO-010 R1 are used for Operational Planning activities only and would not fully define what should fall within the 15 minute adverse impact criteria defined in current NERC CIP Standards which state that only systems that *if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System*.

Xcel Energy does not believe that IRO-010-2 and TOP-003-3 language adequately defines what 'sensitive data' should be included under this new Standard and that a definition of Sensitive Data needs to be created independent of TOP-003-3 requirements or any other Ops & Planning standard.

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 suggests that the drafting team develops a definition for the term "sensitive BES data" something similar to the term "BES Cyber Systems Information" defined for CIP-011. Also, we recommend the definition for the term "sensitive BES data" include language addressing the 15 minute impact operational criteria.

SPP's proposed language for "sensitive BES data"definition:

Data if rendered unavailable, degraded, or misused within 15 minutes would adversely impact the Real-Time operation of the Bulk Electric System.

Our interpretation of the proposed language is that the drafting team has a concern for the protection of the data being transmitted. Since the data being transmitted can't be broken down and identified as sensitive data or non-sensitive data, the recommendation of developing a definition seems to be the safest path. Additionally, we recommend that the drafting team review the term "reliable operation" in the NERC Glossary of Terms. Also, if the term is used in the Requirement, we recommend using the term's definition out of the glossary. Our research shows that this is a defined term and we propose that the term should be capitalized. Finally, we would ask with this being a defined term, does this change the drafting team's intent for the use of this term?

Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	
To promote consistency as the standards change, Reclamation recommends NERC define “sensitive BES data” and “data required for reliable operation” in the NERC Glossary of Terms so that these phrases may be used for all standards (specifically IRO, TOP, and CIP).	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	No
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Great Plains Energy - Kansas City Power and Light Co. - 1,3,5,6 - SPP RE	
Answer	No
Document Name	
Comment	
The case can be made that a requirement to identify, or a definition of, “sensitive BES data” Is not necessary as it is already identified. In consideration of Question 3, we ask another question. The CIP Standards exist to address security risks of the BES to ensure reliability. In order to do that we protect the systems and infrastructure needed to perform the tasks or functions required for BES reliability operating services. Those systems predominately include the data necessary for these functions. “Are the CIP Standards meant to secure more than the data necessary to	

perform reliability tasks? And what gaps, if any, are not addressed or clearly identified in the data deemed necessary to perform reliability obligations in IRO-010-2?"

To protect BES reliability, entities are required under the CIP Standards to protect operational data and BES Cyber Systems Information. This is the same data identified as Real-time monitoring and Real-time Assessment data in IRO-010-2 R1 and TOP-003-3 R1 and R2. Thus the protections may need to be extended to consider Operational Planning Analysis or those data elements that are relevant to promulgate an attack with a longer shelf life of applicability or use.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6

Answer	No
Document Name	

Comment

AZPS disagrees with the SDT's interpretation and asserions relative to broad applicability of the data required for reliable operation under TOP-003-3 and IRO-010-2 to the data contemplated in the directive set forth in Order 822 at paragraph 53. AZPS notes that both TOP-003-3 and IRO-010-2 and the data associated therewith are applicable to the operations planning time horizon and not the real-time operations time horizon. Given the focus of the FERC directive on data in transit between Control Centers during real-time operations, AZPS recommends that the SDT re-evaluate its interpretation as set forth above and assess the need for development of a definition of "sensitive BES data." To scope such definition, AZPS recommends that the SDT reference the definition of Real-Time Assessment in the Glossary of Terms, and those reliability standards that address the performance of Real-Time Assessments and monitoring to identify the data communicated between Control Centers in real-time for performance of such assessments and monitoring.

Further, since each entity has discretion to determine the confidential nature of its data, without a definition, different data could be assigned different levels of sensitivity and confidentiality by different entities. This would create unnecessary ambiguity and complexity for receiving entities – especially where such entity has multiple adjacent Balancing Authorities, Transmission Operators, Generation Operators, etc. AZPS respectfully asserts that, to eliminate inconsistencies and ensure that the real-time data that is critical to reliable operations is uniformly identified and protected amongst all interconnected entities, a definition is necessary.

Finally, AZPS notes that the Guidelines and Technical Basis is not enforceable in finding an entity out of compliance and should be available for supplemental information only. Therefore, while AZPS is not opposed to the provision of guidance, development of a definition for sensitive BES data to be included in the Glossary of Terms is recommended.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
While PJM does agree with the draft language, we feel that it could be tied closely to the CIP-002 assessment (<15 minute impact). For entities that look to the guidance section and chose to use the IRO and TOP standards as a starting point, it should be more apparent that only data used for real-time reliability purposes, that fall within the 15 minute impact, would need to be protected per this standard. It could be mis-interpreted that the guidance suggests protecting all data included in the IRO and TOP standards, even data that may not fall into this real-time category.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
We agree using TOP-003 and IRO-010 Standards to identify data but we believe Operational Planning Analyses data is out of scope. Explicitly stating what data each entity requires in a Standard would not be beneficial. Currently each RC and TOP defines their own requirements for the data that they need from others (per TOP-003-3 and IRO-010). We are concerned that multiple definitions may lead to conflict.	

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We agree with the basic approach of using TOP-003 and IRO-010 Standards to identify this data but needs to be limited to real time data. We believe TOP-003 and IRO-010 include data that is not “real time” so would be outside this document’s scope. An example of data which is out of scope includes data used for Operational Planning Analyses.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
HQT agree, but the reference should be clearly stated. Since IRO-010-2 and TOP-003-3 are future enforceable reliability Standards, the SDT should evaluate the risk of those not being endorsed. If this should happen, the basis would be absent of CIP-012. Also, with the present suggestion, CIP standard would be used to define controls of IRO and TOP standards. This situation could cause an audit gap: the CIP auditors would not have requirement from IRO or TOP to audit against and IRO and TOP auditors would not security requirement to audit against.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
SMUD does not recommend a prescriptive approach. It should be a risk based decision based on the entities risk anaysis.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
The CIP standards are related to protecting BES Cyber Systems and BES Cyber System Information. The Ops and Planning standards are related to other aspects of reliabile operation. Any mixing and matching between CIP and non-CIP standards requirements is an opportunity for confusion, mistakes and potential compliance "double jeopardy".	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	

Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
We agree with the basic approach of using TOP-003 and IRO-010 Standards to identify this data but needs to be limited to real time data. We believe TOP-003 and IRO-010 include data that is not “real time” so would be outside this document’s scope. An example of data which is out of scope includes data used for Operational Planning Analyses.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Yes, Southern Company agrees with the SDT’s approach to utilizing existing Standard requirements that already require the identification of “data and information needed by the RC” to be referenced in the Guidelines and Technical Basis in forming the basis for data transmitted between Control Centers requiring protections in accordance with this Standard. Given the extensive amount of approved and enforceable Standard requirements, as well as those approved for future enforcement, filed with FERC, or under development that are addressing “data exchange via a secure network”, “all data between Control Centers to use a mutually agreeable security protocol”, and “procedures to address the quality of real-time data”, Southern Company agrees that the specific requirements of IRO-010 and TOP-003 sufficiently address the identification of data needing to be protected when transmitted between Control Centers. Any additional attempt to define “sensitive BES data” or to add additional requirements to identify “sensitive BES data” is not necessary.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes

Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
We do not need a clarifier.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
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	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE’s response to #1.	
Likes 0	
Dislikes 0	
Response	

4. The SDT asserts that "availability" of inter-and intra-entity Control Center communication of data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards, specifically Reliability Standards TOP-001-4 and IRO-002-5. The proposed standards require redundant and diversely routed data exchange capabilities at a Responsible Entity's primary Control Center. Do you agree that "availability" is adequately addressed by these standards? If not, please provide rationale to support your position.

Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	

Comment

To promote consistency as the standards change, Reclamation recommends NERC define "availability" in the NERC Glossary of Terms so that the term may be used for all standards (specifically IRO, TOP, and CIP standards).

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

BPA does not agree that "availability" is adequately addressed by redundant and diversely routed data exchange capabilities at the primary Control Center for the following reasons:

1. Currently, the proposed language on page 2 includes protection of "confidentiality and integrity of data required for reliable operation of the BES" and eliminates "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 the requirements of TOP-001-4 and IRO-002-5 (redundancy and diverse routing of data) can be used to achieve increased Availability, it 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 added into the proposed language on page 2 to meet the security objectives of Order 822, i.e., "…to protect AVAILBILITY, 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

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

Answer	No
Document Name	

Comment

CenterPoint Energy does not believe that TOP-001-4 and IRO-002-5 adequately address availability of inter-entity and intra-entity Control Center communication of data. Both Standards speak to data exchange capability having redundant and diversely routed data exchange infrastructure (hardware) once external data enters the primary Control Center. TOP-001-4 and IRO-002-5 do not ensure availability or communication of data between inter-entity and intra-entity Control Centers, but only the redundancy of infrastructure internal to the requesting entity's primary Control Center. Rationale language is specific to this, "Infrastructure that is not within the TOP's primary Control Center is not addressed by the proposed requirement." CenterPoint Energy believes data exchange capability used in TOP-001-4 does not fully address 'data links' between inter-entity and intra-entity Control Centers.

CenterPoint Energy recommends the drafting team re-evaluate "availability" and how it can be adequately addressed by other existing standards.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Tacoma supports the comments of Utility Services, Inc

Likes 0	

Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Yes, Southern Company agrees with the SDT that “availability” is adequately addressed by the other Standards referenced and by common industry practices. Southern Company also offers to the SDT that the only aspect of cyber security at issue under this directive is data integrity. Not only is it appropriate for this effort to be silent regarding availability, we would request that the SDT consider that this Standard should also remain silent regarding “confidentiality.” Including confidentiality will likely result in unintended consequences with no commensurate reduction in risk to BES reliability.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	

Availability is adequately covered by other standards.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
Redundancy and diversity are the primary tools available to support "availability".	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
HQT agree, but the reference should be clearly stated. Since IRO-010-2 and TOP-003-3 are future enforceable reliability Standards, the SDT should evaluate the risk of those not being endorsed. If this should happen, the basis would be absent of CIP-012. Also, with the present suggestion, CIP standard would be used to define controls of IRO and TOP standards. This situation could cause an audit gap: the CIP auditors would not have requirement from IRO or TOP to audit against and IRO and TOP auditors would not security requirement to audit against.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes

Document Name	
Comment	
ERCOT agrees with the SDT's assertion that "availability" is currently addressed by other reliability standards. While TOP-001-4 and IRO-002-5 do address availability, the SDT could cite more of the standards that provide this compliance and enforcement coverage.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Availability is adequately covered by other standards.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP has been generally supportive of the direction the SDT has gone for both TOP-001-4 and IRO-002-5 standard development under project 2016-01.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	

Answer	Yes
Document Name	
Comment	
Availability is already defined in the data specifications of each RC and TOP.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the “availability” of this data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards. We would like to mention to the drafting team that the definition of “Control Center” may need to be re-visited as a result of these new protections. Currently, the definition of “Control Center” may include generation control rooms. We do not believe that these additional protections being proposed by the draft language should be applicable to generation control rooms.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
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	
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	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
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 Austin - AEP - 3,5	
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	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
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	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments in response to this question.	
Likes 0	
Dislikes 0	
Response	

5. The SDT is proposing to develop a new CIP standard because the directives of FERC Order 822 related to the protection of communication networks used to exchange sensitive BES data regardless of the entity's size or impact level. Do you agree with the drafting of a new CIP standard to address this issue? If you disagree and would prefer to include requirements in existing CIP Standards, such as CIP-003 and CIP-005, please provide rationale and propose requirement language.

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

Answer	No
Document Name	

Comment

Any focus on protection of communications networks is misplaced. Protection of data, regardless of the communications medium or network, needs to be the focus of any standards development activities.

Distributed generation, proliferation of smart metering, and ever increasing capabilities in speed and bandwidth of communications technologies are creating new sources of data that can be beneficial in real-time power operations. Entities require innovative mechanisms to securely acquire real-time information into SCADA systems to enable better decision making, whether the data comes via cellular, satellite, leased line, or private carrier connections.

NERC should benchmark with other regulatory bodies which oversee industries with similar needs, such as the financial sector. The financial industry originally used carbon-paper copies of credit cards, submitted to centralized clearing houses, to process credit transactions. Visa provided the first electronic, real-time transaction clearing terminal in 1979. The technologically has proliferated to the point that any smart phone can be used to execute financial transactions in real time. The physical and cyber security of the end points themselves may not be under control of financial institutions. Essentially, what the financial sector has done is provide interfaces to a very sensitive network to millions of devices in real time.

There are many parallels to the power sector, wherein a large quantity of devices increasingly need to send data to control systems over a variety of communications technologies securely, in real-time.

Financial companies have an inherent financial interest in maximizing availability and accessibility of the financial network to increase transactions. Power systems have an inherent reliability interest in getting more information to enable operators to make better real-time decisions.

NERC is in a unique position wherein it may leverage lessons learned from others industries who have decades of experience addressing these types of issues. Any standards development would greatly benefit from cross-pollinization of expertise and not be overly prescriptive so as to limit emerging technologies such a quantum or crypto block chain techniques.

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF

Answer	No
Document Name	

Comment
PJM would prefer to put the language in CIP-005 for Highs and Mediums and CIP-003 for Lows.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
Duke Energy disagrees with the drafting of a new standard to address this directive. We feel that based on the current draft language, this requirement would be better suited in CIP-003-3. Adding to an already existing framework rather than creating a new standard is preferable. Creating a new standard would also require an entity to create additional documentation, rather than adding to already existing documentation.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment
We believe that protection of communications networks would best be incorporated into existing CIP-005 or CIP-011 Standards.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	
Comment	

SRP disagrees with the proposition to develop a new CIP standard. SRP suggests keeping requirements for low impact systems in CIP-003. Since CIP-005 already protects the BCS up to the point of EAP, it is possible to add another requirement to protect “BES sensitive data” between EAPs via site to site encryption, application layer encryption, or physical protections (as described in the “Draft Guidance” section). In addition to CIP-003 and CIP-005, the SDT should consider modifying CIP-006 R1.10, which includes requirements to protect cabling and other nonprogrammable communication components, to ensure no conflicts.

SRP prefers a risk-based approach that has different requirements for high, medium, and low impact systems.

Likes 0	
Dislikes 0	
Response	

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	
Comment	

If the objective is to provide protection of the telecommunications interface or boundaries at control centers, it appears this is already addressed under CIP-002 and CIP-006. Clarifying language for existing standards would be sufficient to address protection issues.

Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3,4,5, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	
Comment	

The existing cyber security controls in CIP-003 and CIP-005 already provide the basis for the protection of the communication links between control centers. It is better to enhance these requriements to include the communication links then a new requirement

Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG recommends maintaining the current Standards (CIP-003, CIP-005, CIP-006, CIP-007, and CIP-011) and revise them accordingly or as needed to protect the data. These particular Standards have the potential to address the concerns pertaining to sensitive BES data, regardless of the entity's size or impact level. Also, they can reduce the potential of creating redundancy issues.	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
If the SDT develops a new CIP standard it could be difficult for an entity to know which standard to apply if there is any overlap between existing standards and thus the preference would be to incorporate any new requirements into CIP-003 and CIP-005.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

In isolation, it might be less confusing to group the new requirements together; however, the continued addition of new standards, attachments, etc. has made the standards increasingly difficult for Responsible Entities to fully understand and comply with. If these new requirements are necessary, IPC suggests adding them to CIP-005-5 as R3 with associated parts since CIP-005-5 deals with ESP boundaries and external connections.

Likes 0	
Dislikes 0	

Response

Aaron Austin - AEP - 3,5

Answer	No
Document Name	

Comment

Requirements for communications to high and medium impact BCS should reside in the location with the other electronic access requirements in CIP-005. Similarly, the requirements for communications between low impact BCS at control centers should reside with the other requirements for low impact BCS written comenserate with the risk. There should be a “high water mark” provision to protect communications from low impact BCS at control centers to high and/or medium impact BCS at control centers.

Likes 0	
Dislikes 0	

Response

Guy Andrews - Georgia System Operations Corporation - 3,4

Answer	No
Document Name	

Comment

If the SDT develops a new CIP standard it could be difficult for an entity to know which standard to apply if there is any overlap between existing standards and thus the preference would be to incorporate any new requirements into CIP-003 and CIP-005.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
CIP-005 is used to define the network compliance controls. Spreading network compliance controls throughout different CIP could result in confusion in the application of the different required controls. The CIA requirements for data (in transit or at rest) should be explicitly defined in CIP-005.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA does not agree that a new standard is required. A new standard could result in isolated requirements that do not blend with – or even contradict – existing requirements. The objectives can be met by coordinating with existing standards such as CIP-003 & CIP-005.

BPA also proposes that the Guidelines and Technical Basis section should emphasize that entities can/should leverage evidence from the numerous other CIP standards where data quality, confidentiality and availability is also addressed.

Potential language to be incorporated into CIP-005-x R3:

Applicable Systems: High Impact BES Cyber Systems at Control Centers; Medium Impact BES Cyber Systems at Control Centers

Requirements: R3. The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect availability, confidentiality and integrity of data required for reliable operation of the BES. The plan applies to data being transferred across communication networks between Control Centers, both inter-entity and intra-entity and shall include each of the applicable requirement parts in CIP-005-x Table R3.

3.1 Identify data required for reliable operation of the BES (if not already identified under IRO-010-2 and TOP-003-3).

3.2 Where technically feasible, have one or more methods for protecting availability, confidentiality and integrity of the data identified in 3.1.

3.3 Have one or more methods for alarming to a central location when loss of protection of data failed to a central location with a method of immediate response.

3.4 Have one or more methods for timely response to alarms identified in 3.3.

Potential language to be incorporated into the next version of CIP-003-x, R1.2, For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any: *New:* 1.2.7. Ensuring the availability, confidentiality and integrity of data required for reliable operation of the BES between Control Centers, both inter-entity and intra-entity.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
No – utilize existing standards. The impact level should be considered within the the context of existing standards.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	No
Document Name	
Comment	
It may be impossible to protect the "networks". It is more important to ensure the availability, confidentiality and integrity of the data flowing over those networks. As previously noted, redundancy and diversity, along with monitoring, are tools which can ensure availability, and can be addressed in the ops & planing standards. Properly implemented encryption, is a tool which can ensure confidentiality and integrity of the data and can be addressed within CIP-005.	
Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
Xcel Energy believes a new Standard is not required to address the risks identified in FERC Order 822. Xcel Energy believes that existing CIP-003 and CIP-005 standards should be updated as determined necessary to address the concerns identified in the order. Current CIP Standards include a comprehensive set of requirements to protect the Bulk Electric System and specific controls to address new risks should be integrated into existing requirements when possible. Creating a new standard would add unnecessary complexity and lead to confusion when it may include requirements already covered by CIP-003, CIP-005, CIP-006 and potentially CIP-011. The development of a new Standard to address this concern without coordination of existing CIP requirements would also create an unknown and complex audit approach with risk of creating instances of double jeaproady that could otherwise be prevented with proper integration and revisions of current CIP Standards to address the concern.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
We recommend maintaining the current Standards (CIP-003, CIP-005) and revising them accordingly or as needed. These particular Standards have the potential to address the concerns pertaining to sensitive BES data regardless of the entity's size or impact level. Also, they can reduce the potential of creating redundancy issues.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	No
Document Name	
Comment	

Reclamation recommends the requirements for protecting communication networks should be included in CIP-003-7i for low impact BES Cyber Systems; and CIP-005-5 for the high and medium BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC

Answer	No
Document Name	

Comment

Southern Company disagrees with this approach and respectfully requests the SDT to consider the technical and procedural controls that result from these new requirements will almost certainly be designed, implemented, and maintained in conjunction with the controls in CIP-005 (for Highs and Mediums) and CIP-003 (for Lows). Rather than create a new set of requirements, guidance, RSAWs, etc. for something that will have to be audited along with and as if it were a part of CIP-005 (for Highs and Mediums) or part of CIP-003 (for Lows), we would recommend modifying those Standards.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6

Answer	No
Document Name	

Comment

Basin Electric would prefer low impact requirements be kept in CIP-003 as this minimizes potential confusion with low impact level only entities. Basin Electric would prefer additions to CIP-005 vs. a new standard as the protections for high and medium impact levels would be closely tied to an Electronic Security Perimeter and crossing the applicable boundary for a Control Center.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS can see the value in the development of an entirely new standard; however, AZPS is concerned that the development of an entirely new standard is beyond the scope of the FERC directive, which states that “modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability.” Therefore, AZPS requests that the SDT evaluate and clarify whether the SAR provides the additional authority necessary for the development of a new standard, as opposed to the modification of CIP-006-6.	
Likes 0	
Dislikes 0	
Response	

Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	No
Document Name	
Comment	
If the objective is to provide protection of the telecommunications interface or boundaries at control centers, it appears this is already addressed under CIP-002 and CIP-006. At most this would require some clarifying language.	
Likes 0	
Dislikes 0	
Response	

sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	

Per the NSRF: If the objective is to provide protection of the telecommunications interface or boundaries at control centers, it appears this is already addressed under CIP-002 and CIP-006. Clarifying language for existing standards would be sufficient to address protection issues.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
A new standard will assist in defining the requirements addressing the inter-relationship between entities of differing impact levels.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes

Document Name	
Comment	
The Standard Drafting Team's proposed approach seems consistent with the discussion in FERC Order No. 822 delineating between the CIP Standards focusing on "boundary" issues – that is, the definition of boundaries and the creation of protections at those boundaries – and the data security and communication link issue for BES sensitive data being transmitted across such boundaries.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
There are concerns about the applicability section and how it will interact with the existing CIP Standards exemption 4.2.3.2. The applicability section should limit the scope to only real time communication networks or data between Control Centers. Would like additional guidance on the applicability of technologies like voice communication email, text messaging … Consider including language for CIP Exceptional Circumstances	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Since these requirements are not limited to just communications between entities at the same impact level, a new standard will assist in defining the requirements that address the interrelationship between entities of differing impact levels.	

Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
A new standard would be less disruptive. This way all policy/procedure changes would be contained in 1 document.	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
A new standard would be preferred to specify the communication network requirements.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Because of the way SCE has organized the assignment of CIP requirements into Programs, this has no impact to us operationally. SCE believes the general benefit of creating a new CIP standard (CIP-012) is that like requirements would be grouped together and easier to locate.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
The requirements span multiple impact levels and a new standard would assist entities in identifying the applicability of the new requirements.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	

Comment	
Request the SDT consider and address how existing CIP Standards exemption 4.2.3.2 could be impacted. There are concerns about the applicability section and how it will interact with the existing CIP Standards exemption 4.2.3.2. The applicability section should limit the scope to only real time communication networks or data between Control Centers. Would like additional guidance on the applicability of technologies like voice communication email, text messaging. Consider including language for CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	

Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 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	

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
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	

6. The SDT evaluated multiple approaches to addressing the directive. The approach proposed in this informal posting focuses on the protection of communication links. An alternative approach could focus on the protection of the sensitive BES data itself. Do you agree with the SDT's approach to focus the draft language on the protection of communication links? If not, please provide rationale and propose alternative language.	
sean erickson - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
What you are trying to protect data/link/network will ultimately determine how best to protect it, and it is not clear from this request what that is. per the NSRF: The NSRF recommends focusing on the boundaries or interface points, not the links between control centers.	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	No
Document Name	
Comment	
We agree with focusing on the boundaries or interface points, not the links between control centers.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	

Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS does not agree that protection of the communication links alone achieves the FERC directive, which also references controls to protect the data communicated between BES Control Centers. Controls that would be applicable to the protection of data include controls such as encryption, which is different and superior to the controls that would be used to protect communication links alone.	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
Basin Electric prefers objective based standards/requirements. If the objective can be met via multiple methods (e.g. protected communication links or protecting the data itself), Basin Electric would prefer the flexibility to choose the approach and method. The proposal does include flexibitily within the protection of communication links approach which is appreciated.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	

Answer	No
Document Name	
Comment	
Reclamation recommends including requirements for protecting communication networks in CIP-003-7i for low impact BES Cyber Systems, in CIP-005-5 for high and medium BES Cyber Systems, and in CIP-006-6 Requirement R1 Part 1.10 for physical security.	
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 review group recommends working on a multiple approach solution to address the directive. The Primary Solution could address the protection of the communication link. As an alternative method, we recommend the drafting team consider other methods that are not link level controls. Additionally, we would ask the drafting team to provide clarity on the difference between “communication links” and “communication networks”.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
The SDT should continue to evaluate multiple approaches to address the directive. Allowing the entity to determine which is appropriate based on situation. It might not be feasible to always implement link controls between entities.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	No
Document Name	
Comment	
Rather than focusing on the links, we should focus on protecting the data. If that means implementing certain protections such as encryption over the links, that's fine. Don't focus on the links themselves.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	No
Document Name	
Comment	
No – SMUD requests that the definition of communication links should be clarified.	

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

BPA does not agree that focusing on protection of the communication links is the best approach to meet the FERC directive. Merely protecting the network, or communications links, does not necessarily protect the data carried by the network. However, if the requirement instead emphasizes protection of data, BPA believes entities will gain the additional benefit of creating a more secure cyber environment overall.

BPA proposes that draft language be revised to require method(s) for protecting “applicable data” rather than “communication links” between Control Centers.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The strategy of protecting the sensitive BES data itself is a better one than to focus on wether the data is at rest or in-transit. The CIA objectives could be added to CIP-005 & CIP-011. This would maintain the current consistency and approach of the CIP standard.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT does not agree with protection of communication links. The requirement should be written to allow entities to implement the program that fits their needs and infrastructure. Some may be best suited to protect the data and others may be best suited in protecting the communication links. The security objects should remain as it is with options in how to achieve the objective as articulated in the draft guidance.	
Likes 0	
Dislikes 0	
Response	

Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
Either of the two approaches could provide good security measure but why limit the entity to only one approach. It would be better to allow each entity to choose their own approach which best fits their environment.	
Likes 0	
Dislikes 0	
Response	

Aaron Austin - AEP - 3,5	
Answer	No
Document Name	
Comment	
AEP believes the security directive for the requirements should be written in a way to permit any responsible entity to achieve the directive, regardless of technology or preferred architecture.	
Likes 0	

Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
Either approach of protecting the data or the communication links should be an option for a Responsible Entity as long as the Responsible Entity meets the security objective of providing confidential data that has integrity.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. The Standard should be an outcome based Standard. FERC Order 822 section 58 clarifies this scope as inter-Control Center and intra-Control Center communications. The guidance seems to extend the scope beyond this by including references to DP's and listing Data links without reference to Control Centers.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	

Comment
Either of the two approaches could provide good security measure but why limit the entity to only one approach. It would be better to allow each entity to choose their own approach which best fits their environment.

Likes 0	
Dislikes 0	

Response

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

Comment
Texas RE suggests that the suggested requirements could be more clear. FERC Order No. 822, P. 56 provides that "NERC's response to the directives in this Final Rule should identify the scope of sensitive bulk electric system data that must be protected and specify how the confidentiality, integrity, and availability of each type of bulk electric system data should be protected while it is being transmitted or at rest." Elsewhere, FERC Order No. 822 specifically refuted reliance on the EOP-008-1 Standard because that Standard "does not provide for the protection of communication links and sensitive bulk electric system data communicated between bulk electric systems Control Centers." FERC Order No. 822, P. 63. In short, FERC Order No. 822 appears to specifically contemplate protections for both communications links and electric system data as separate categories. On page 4 of the Unofficial Comment Form, the Standard Drafting Team (SDT) notes that "the Responsible Entity must document and implement plans for the protection of the confidentiality and integrity of operational reliability data communicated between Control Centers." The SDT then references examples of methods to protect data, such as site to site encryption and application layer encryption. Texas RE believes these are appropriate examples of methods to protect electric system data that is consistent with the intent of FERC Order No. 822. However, Texas RE is concerned that the SDT's proposal potentially subsumes these data-focused protection methods under protections for physical communications links themselves. Although such protections are appropriate, FERC Order No. 822 appears to view data security and physical communications link protections as separate, augmentative elements of a robust data security program. As such, Texas RE recommends that the SDT further specify that in order to achieve the security objective to protect confidentiality and integrity of data required for the reliable operation of the BES, responsible entities include the following language: **1.4 Method(s) for protecting the operational reliability of data communicated between Control Centers identified in 1.1, where technically feasible.**

Likes 0	

Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG likes the approach of protecting communication links because you can identify the data, but at what point does the data transfer ownership from the responsible entity to the RC or BA (therefore, NRG also recommends that the SDT also definine the data to be protected). From that standpoint, additional requirement protections to be added into CIP-005 are recommended (by NRG) to protect the confidentiality and integrity of the data. NRG recommends working on a multiple approach to address the directive. The primary solution could address the protection of the communication link. As an alternative method, NRG recommends that the drafting team consider other methods that are not link level controls. Additionally, NRG asks that the drafting team provide clarity on the difference between “communication links” and “communication networks”.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	No
Document Name	
Comment	
As written, it is unclear what constitutes a “communication link”, especially if that link is provided by a 3rd party. The standard should address the protection of the data.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	

Comment
The NSRF recommends focusing on the boundaries or interface points, not the links between control centers.

Likes 0	
Dislikes 0	

Response

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

Comment
SRP does not agree with the SDT's approach to focus the draft language on the protection of communication links. The focus of the draft language should be on both the communication links and the sensitive BES data, as required by FERC Order No. 822. The reliability of the communication links and integrity of sensitive BES data are critical to the reliability of the BES. SRP proposes merging the language that focuses on protection of communication with the language in the "Draft Guidance" section pertaining to the data-centric approach.

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	No
Document Name	

Comment
1. Recommend that the SDT focus on protecting the data for reliability and availability. 2. We recommend that this Standard not prescribe the method for protecting the data but the objective of reliability and availability as the focus. Alternative approaches of application security or communication security controls should be allowed and clearly addressed in the Requirements. The proposed procedures in Draft Language 1.1 and 1.2 would not be required.

3. FERC Order 822 section 58 clarifies this scope as inter-Control Center and intra-Control Center communications. The guidance seems to extend the scope beyond this

4. Recommend reviewing NIST Special Publication 800-47 which is titled Security Guideline for Interconnecting Information Technology Systems with a focus toward reliability and availability

5. The Standard should be an outcome-based Standard.

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

Supporting APPA comments

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 1,3,4,5,6

Answer	No
Document Name	

Comment

This requirement should be drafted to allow Responsible Entities to implement an approach which fits the needs of its processes and infrastructure; allowing for either data and/or communication link protection.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
TVA notes that within a cloud-based communications network such as the Internet, an MPLS network, a meshed network, or other non-point-to-point type of communications topology, it would be difficult to quantify a “link” as a physical or logical construct, as the “link” may be constructed of a virtual circuitry that traverses any number of underlying physical components. The language should be revised to focus on protecting information instead of antiquated notions of physical communication components associated with “links.” TVA is also concerned that the proposed language is vague enough to encompass transport links carrying an e-mail sent between two Control Centers, as no qualifications are provided regarding timeliness of the information. Should Internet based transport relay the e-mail, the registered entity would be obligated to protect, end-to-end, the Internet “data-links” connecting the two Control Centers. TVA suggests focusing on the “sensitive bulk electric system data” moving between Control Centers and not underlying communications infrastructure.	
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	
We support a path forward of focusing on protection of communication links with language to limit the scope of data to be protected with that data that does not have a shelf life or is considered perishable.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	

Comment
Yes, Southern Company supports the SDTs approach focused on protection of communication links between Control Centers. Additionally, Southern requests the SDT to consider the providing clarifying language that ensures the proper scoping of this Standard to be “communications between Control Centers” and exclude their associated data centers. The definition of Control Center could inadvertently require additional protections be afforded to communications between an entity’s Control Centers and it’s own data centers, and that does not appear to be the intent stated in the FERC Order.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	

Comment
See attachment Q1

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	

Comment
AECI agrees with the SDT's approach that the focus should be on the communication links rather than the sensitive BES data itself.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	
Comment	
It is likely that the same types of logical controls would be utilized to protect either. It would be best to further the already established concept of protecting communication networks/links and explain how that, in turn, protects the data.	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
We agree with the approach to focus the draft language on the protection of the communication links. If the SDT decides to focus on the sensitive BES data, then a definition for “sensitive BES data” would need to be developed. The applicable requirements in IRO-10-2 and TOP-003-3 do not adequately address this.	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Perhaps the language should be edited in a manner that will allow entities to protect links and/or the sensitive BES data itself, allowing entities flexability in achieving the security objective.	
Likes 0	
Dislikes 0	

Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the approach that the focus of the protection should be on the communication links rather than the sensitive BES data itself.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CenterPoint Energy agrees that the focus should be on the protection of the communication link used to transport sensitive BES data and not the sensitive BES data itself. This aligns with the language in the FERC order “to require responsible entities to implement controls to protect, at a minimum, all communication links and sensitive bulk electric system data communicated between all bulk electric system Control Centers.”(FERC Order 822, P.41)	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
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	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
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	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	
Document Name	
Comment	

1) Recommend that the SDT focus on protecting the data for reliability and availability

2) We recommend that this Standard not prescribe the method for protecting the data but the objective of reliability and availability as the focus. Alternative approaches of application security or communication security controls should be allowed and clearly addressed in the Requirements. The proposed procedures in Draft Language 1.1 and 1.2 would not be required.

3) FERC Order 822 section 58 clarifies this scope as inter-Control Center and intra-Control Center communications. The guidance seems to extend the scope beyond this

4) Recommend reviewing NIST Special Publication 800-47 which is titled Security Guideline for Interconnecting Information Technology Systems with a focus toward reliability and availability

5) The Standard should be an outcome based Standard. We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. The Standard should be an outcome based Standard. FERC Order 822 section 58 clarifies this scope as inter-Control Center and intra-Control Center communications. The guidance seems to extend the scope beyond this by including references to DP's and listing Data links without reference to Control Centers.	
Likes 0	
Dislikes 0	
Response	

7. Do you agree with the security objective of the draft language? If not, please propose alternative language.

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

Answer	No
Document Name	

Comment

It is the Entity's responsibility to protect its information systems, regardless of the origin of information that is fed info an information system. Specifically, the draft Guidance language directs REs to establish controls for data links between DPs and TOPs. In such a scenario, the DP may not be subject to any regulatory controls and the TOP has no mechanism to enforce what a DP is doing with their end of a communications link. Accordingly, the TOP is powerless to enforce end-to-end data link protections required by the draft language.

In the event that an RE has the ability to control data-link security end-to-end with other entities, such a protection still provides no inherent cyber security benefit for the information carried over the data link; the information itself may contain a malicious payload carried over an otherwise trusted data-link.

It is incumbent upon REs to configure information systems under their control to ensure that information provided to information systems is safe, trustworthy, and appropriately vetted; and potential for adverse impact of incomplete, untrustworthy, or malicious data has been appropriately mitigated. For example, on a Microsoft Windows server, the RE may install security patches that were downloaded from the public Internet. Such information is potentially adversely impactful to a BES Cyber System. However, the entity takes appropriate action to ensure the security patches are genuine. Even though communications links utilized for the vast majority of the transport are untrustworthy, appropriate application layer controls are leveraged to ensure the trustworthiness of the communications payload.

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

Supporting APPA comments

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	No
Document Name	
Comment	
PJM proposes that the objective should focus on protecting the communication networks. Proposed language: “The Responsible Entity shall implement one or more documented plan(s) to protect data being transferred across communication networks between Control Centers, both inter-entity and intra-entity that include each of the applicable parts below:” The “Purpose” should include the security objective (confidentiality and integrity of data required for reliable operation of the BES).	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy does not disagree with the security objective to protect confidentiality and integrity of data required for reliable operation of the BES. We do not agree that the current draft language is measurable, and thus would make it difficult to audit. Moreoever, the draft language does not appear to fit the mold of other standards which are performance based. Also, more descriptive language needs to be placed in the requirement. Currently, as written, an entity would need to refer to the Guidelines and Technical Basis section to determine what was necessary to comply.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	No
Document Name	
Comment	

We suggest "reliability and availability" replace "confidentiality and integrity" because EMS/SCADA systems are built on "reliability and availability." There should be flexibility when it comes to enforcing encryption and specifying methods and end points.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC

Answer	No
Document Name	

Comment

The security objective should be to protect the data.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The security objective is not clearly stated. We recommend the drafting team put more emphasis or focus on the integrity of the data instead the confidentially. Additionally, we recommend a definition of data to be protected such as: Data if rendered unavailable, degraded, or misused within 15 minutes would adversely impact the Real-Time operation of the Bulk Electric System. Does this mean that everytime you do a database change, that change control per the CIP standards must be utilized? (for example, if the database is degraded, it may have a 15 minute impact).

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	
Comment	
Propose deleting reference of confidentiality in the standard and focus on integrity because adding confidentiality expands the scope of the FERC Directive.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
We suggest “reliability and availability” replace “confidentiality and integrity” because EMS/SCADA systems are built on “reliability and availability”.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	No
Document Name	
Comment	
Propose deleting reference of confidentiality in the standard and focus on integrity because adding confidentiality expands the scope of the FERC Directive.	
Likes 0	
Dislikes 0	
Response	

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
The commission is asking to implement controls to protect, at a minimum, the communication links and the data being communicated. The concepts introduced by the SDT (Confidentiality, Integrity, availability), are valid, but are not directly required by the commission. Also, the current CIPs do not mention those concepts. Either the requirements of the commission are updated or the SDT should fallback to the commission language.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
In regards to the objectives, confidentiality and integrity have not been stated as explicit objectives in the current Standards, although they are obviously implied. The security objective should align with the current standards – “to protect against compromise that could lead to misoperation or instability in the BES.”	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
The language regarding physical security in the guidance section is concerning to Xcel Energy as physical security is not specifically referenced in the Standard or Requirement language. Cabling within an ESP spanning multiple PSPs is already required to be physically secured (or deploy alternative	

measures such as encryption) under CIP-006-6 R1.10, so requiring this on all wiring would greatly increase the scope of cabling beyond what is needed under CIP v6. If the SDT/FERC believes that all cabling in Control Centers need to be physically protected, then Xcel Energy would suggest the SDT update the existing language in CIP-006-6 R1.10 instead of through a new, separate, standard which raises the concern of double jeopardy and adds a new "spaghetti" requirement previously done away with by v5/v6. Xcel Energy suggests that the word 'confidentiality' be removed from draft language "*The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect* ***confidentiality*** *and integrity of data required for reliable operation of the BES"* to ensure consistency throughout the other CIP standards.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
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 security objective is not clearly stated. We recommend the drafting team put more emphasis or focus on the integrity of the data instead of the confidentially. Additionally, we recommend a definition of the data to be protected such as: Data if rendered unavailable, degraded, or misused within 15 minutes would adversely impact the Real-time operation of the Bulk Electric.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
We suggest “reliability and availability” replace “confidentiality and integrity” because EMS/SCADA systems are built on “reliability and availability”.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS does not agree with the security objective of the draft language as it is overly broad and extends beyond the scope of the directive set forth in Order 822 at Paragraph 53, which specifically targets data in transit between Control Centers. To the extent that this language is retained, AZPS recommends that the security objective be revised to state: “…achieve the security objective to protect confidentiality and integrity of data communicated between bulk electric system Control Centers and the associated communication links…”	
Likes 0	
Dislikes 0	

Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No
Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the security objective of protecting the confidentiality and integrity of data that is required for reliable operation and is transmitted between Control Centers.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
If the security objective is to protect the confidentiality and integrity of operational reliability data transmitted between control centers, the NSRF agrees	
Likes 0	

Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
As it is understood, the objective is to ensure that data transmitted is received in a way that the recipient can be confident the data is complete and accurate.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
In meeting the security triad of confidentiality, integrity, and availability, the security objective for availability is already addressed and monitored as noted under question 4. This requirement should be limited to the remaining two objectives of integrity and confidentiality.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

BPA agrees with the security objective but suggests that the supporting language needs to be modified to support the objective of protecting data rather than emphasizing protection of communication links. As discussed above, BPA also encourages the SDT to incorporate the requirements into existing CIP standards rather than creating a new standard. Wherever the requirements reside, BPA proposes the following edits to the draft SDT language:

The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect availability, confidentiality and integrity of data required for reliable operation of the BES. The plan applies to data being transferred across communication networks between Control Centers, both inter-entity and intra-entity and shall include each of the applicable parts below:

1.

i. *Identification of the data required for reliable operation of the BES (if not already identified under IRO-010-2 and TOP-003-3);*

ii. *Method(s) for protecting applicable data between Control Centers identified in 1.1, where technically feasible.*

iii. *Loss of protection of data should be alarmed to a central location with a method of timely response.*

Likes 0	
Dislikes 0	

Response

Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF

Answer	Yes
Document Name	

Comment

Yes, the primary objective should be on protecting the data.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment	
Reclamation recommends adding the draft language to CIP-003-7i for low impact BES Cyber Systems, to CIP-005-5 for high and medium BES Cyber Systems, and to CIP-006-6 Requirement R1 Part 1.10 for physical security.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the security objective of the draft language, but as previously stated, believes the language including the requirement to demonstrate confidentiality be removed. Although confidentiality is part of the foundational CIA security triad, in most instances confidentiality does not have a real-time (<15 minute) impact to the reliability of the BES.	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	

Answer	Yes
Document Name	
Comment	
If the security objective is to protect the confidentiality and integrity of operational reliability data transmitted between control centers, we agree.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 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	
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	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
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	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
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	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	

8. Is it clear what types of plans, procedures, and methods are needed to meet the draft language? If not, please propose alternative language.

sean erickson - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

Referring to the protection of communication links, does this mean select individual links or does it really mean an entire network?

per the NSRF:The question assumes the development of a new standard. The NSRF believes the objectives can be met through simple clarifying language in CIP-002 and CIP-006. We believe the intent of the Order is met though other changes that have occurred in the standards over time. Confidentiality is appropriately addressed through the NERC ORD Confidentiality Agreement. The integrity of data is also addressed in multiple standards dealing with managing the quality of data used by operators (there are 136 references to data quality in the current set of standards).

Likes 0	
Dislikes 0	

Response

Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2

Answer	No
Document Name	

Comment

The question assumes the development of a new standard. We believe the objectives can be met through simple clarifying language in CIP-002 and CIP-006. We believe the intent of the Order is met though other changes that have occurred in the standards over time. Confidentiality is appropriately addressed through the NERC ORD Confidentiality Agreement. The integrity of data is also addressed in multiple standards dealing with managing the quality of data used by operators (there are 136 references to data quality in the current set of standards).

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	Project 2016-02 Communication Networks - Comment for Question 8.docx
Comment	
Please see the attached document for AZPS' comments regarding Question 8.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
We do not agree with the draft language which focuses on networks. This language should focus on data. We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. Replace “communication networks” with “communication networks or BES reliability data”. Include in 1.1 that this is for networks or data between Control Centers.	
Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	
Answer	No
Document Name	
Comment	
This question can only be answered once a determination has been made as to whether a new standard is going to be created or updates are made to existing standards.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	No
Document Name	
Comment	
A CIP-005 requirement for physical protection or encryption of data flowing between ESPs associated with High and/or Medium Impact BES Cyber Systems should be sufficient to address this need.	
Likes 0	

Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
The openness left to entities allows flexible solutions that would be more appropriate than prescriptive requirements would allow. This flexibility leaves concerns to what degree it would be audited to, this is similar to the Low Impact requirements.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. Replace “communication networks” with “communication networks or BES reliability data”. Include in 1.1 that this is for networks or data between Control Centers.	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	

Comment
Please see Texas RE's comment in response to Question 6.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC

Answer	No
Document Name	

Comment
Delete 1.1 1- Define the boundaries of communication networks transmitting data required for reliable operations. 2- Method(s) for protecting the in scope data between Control Centers where technically feasible.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	No
Document Name	

Comment
The question assumes the development of a new standard. The NSRF believes the objectives can be met through simple clarifying language in CIP-002 and CIP-006. We believe the intent of the Order is met though other changes that have occurred in the standards over time. Confidentiality is appropriately addressed through the NERC ORD Confidentiality Agreement. The integrity of data is also addressed in multiple standards dealing with managing the quality of data used by operators (there are 136 references to data quality in the current set of standards).

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	No
Document Name	
Comment	
Language should focus on data, not networks. There should be flexibility when it comes to enforcing encryption and specifying methods and end points.	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy suggests the drafting team consider the balance between existing CIP requirements, and the proposed requirement to protect and encrypt communication paths. There are existing CIP requirements in CIP-005-5 that certain communications links be inspected for malicious code for inbound and outbound communications. If a communication link is now expected to be encrypted, the ability to inspect the traffic for malicious code will not be feasible. If an entity determines that encryption is therefore not a possible option to be able to maintain compliance with existing requirements, the only suggested protection mechanism left would be physical and is not feasible in most situations.	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy has concerns with implementing methods for protecting communication links between Control Centers (R1.3) in situations where the end point is not owned by the entity. What would be the compliance implications if the owner of the end point is not willing to implement	

protections? CenterPoint Energy recommends that the drafting team provide guidance around ownership of communication links and how to comply with the requirement in these situations.	
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	
Supporting APPA comments	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The responsibilities assigned to REs potentially cover information systems for which the RE has no control, creating compliance obligation that would be impossible to satisfy.	
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
We also believe sub Requirements 1.1 and 1.2 look as if they can be consolidated. Proposed language follows at the end of this response. Possible Alternative Language: **R1.** The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect confidentiality and integrity[1] of data required for reliable operation of the BES. The plan applies to data being transferred across communication networks between Control Centers, both inter-entity and intra-entity and shall include each of the applicable parts below: **R1.1** Procedure(s) to identify networks requiring protections, and their associated boundaries. **R1.2** Procedure(s) to associate the categorization completed under CIP-002-5.1a with the identified networks in R1.1. **R1.3** Procedure(s) to design, construct, and implement protections for the networks identified in R1.1. The procedure shall be tailored to address the high, medium, and low impact risks associated with the networks in R1.2. **R1.4** Procedure(s) to address protections for networks identified in R1.1 where technically feasible. [1] NIST Special Publication 800-53A : Revision 4, Appendix B (Glossary) **[NIST incorporates by reference the definition found in U.S. Code, Coordination of Federal Information Policy, Information Security (44 U.S.C. §3542), defining "integrity" as "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."**]

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	Yes
Document Name	

Comment
Basin Electric would prefer the plans, procedures and methods be included in CIP-003 and CIP-005 as appropriate vs. in the new proposed standard CIP-012.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See attachment Q1	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
For requirement 1.3, we recommend adding the bulleted list from the Draft Guidance Section (similar to CIP-006-6 R1.10) into the requirement language. The requirement would be written as follows: **1.3** Method(s) for protecting communication networks between Control Centers identified in 1.1, where technically feasible. The Responsible Entity shall document and implement one or more of the following: • Site to site encryption; or • Application layer encryption; or • Physical protections.	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment	
ERCOT requests that the SDT also consider guidance on where parties at either end of a communication link are not in agreement.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
It is important to maintain flexibility for Responsilbe Entities to develop controls that work best within their environment and for their situation. The less prescriptive the requirements, the more flexible and agile the Responsible Entity can be to work within the skills sets of their personnel and respond to the changing security and technology landscapes. IPC suggests that the requirements state objectives and requirements to document positions and controls and be less prescriptive than the CIP standards are in their current state.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
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	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

9. The SDT uses the term “communication networks” throughout the draft language including an obligation to define the boundaries of such communication networks. Does the SDT need to define the term for inclusion in the NERC Glossary of Terms? If so, please propose a definition of “communication networks.”

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

Supporting APPA comments

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

CenterPoint Energy recommends using the term “communication link(s)” instead of “communication networks” in the requirement language to align with the FERC directive. The term “communication networks” can encompass many types of networks, some of which are currently out of scope for the CIP Standards. CenterPoint Energy believes the focus should be on the protections around the communication links used to transmit sensitive bulk electric system data between Control Centers. CenterPoint Energy recommends the following changes:

*“The Responsible Entity shall implement one or more documented plan(s) that achieve the security objective to protect confidentiality and integrity of data required for reliable operation of the BES. The plan applies to data being transferred across communication **links** between Control Centers, both inter-entity and intra-entity and shall include each of the applicable parts below:*

*1.1 Procedure(s) to identify the communication **links** requiring protections;*

*1.2 Procedure(s) for defining the boundaries of communication **links** transmitting data required for reliable operation identified in 1.1, if applicable;*

*1.3 Method(s) for protecting communication **links** between Control Centers identified in 1.1, where technically feasible.”*

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	No
Document Name	
Comment	
PJM asserts that “between Control Centers” already clarifies the scope.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1,3,5,6, Group Name Con Edison	
Answer	No
Document Name	
Comment	
CIP-002 Exemptions already utilize the "communications networks" term. However, consider that the FERC Order Section 58 clarifies the focus and the scope on inter-Control Center and intra-Control Center communications	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Draft language, applicable part 1.1 call for procedure(s) to identify the communications network requiring protections. A defined term for communication network may restrict an entity’s flexibility in determining how to implement the draft language.	
Likes 0	

Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
The term "communication networks" is used elsewhere in the standards. The NSRF believes that defining the term for one standard would have unintended impacts on other standards.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4	
Answer	No
Document Name	
Comment	
Does not need to be defined, because from a simple view it includes everything outside the CIP ESP.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7,8 - WECC	
Answer	No
Document Name	
Comment	

The standard uses two terms; "communication networks" and "communication links". Use one term, not two. We believe the standard should address securing the data, not the "networks" or "links".	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Recommend a NO vote on defining “communication network” But consider that the FERC Order Section 58 clarifies the focus and the scope on inter-Control Center and intra-Control Center communications	
Likes 1	Illinois Municipal Electric Agency, 4, Thomas Bob
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
The term “communication networks” is used elsewhere in the standards. The NSRF believes that defining the term for one standard would have unintended impacts on other standards.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC,SPP RE	

Answer	No
Document Name	
Comment	
The term communication Networks has many different applications and is too broad of a term to be used in in Standard Language without adding a defined term in the NERC Glossary. The FERC directive only references “Links.” Xcel Energy would suggest formal definitions be drawn up for both Communication Networks and Links.	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1,3,5,6	
Answer	No
Document Name	
Comment	
The term "communication networks" is already used in the applicability section of the CIP standards. Defining this term could have unintended consequences.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
Recommend a NO vote on defining “communication network”. But consider that the FERC Order Section 58 clarifies the focus and the scope on inter-Control Center and intra-Control Center communications.	
Likes 0	
Dislikes 0	

Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - NA - Not Applicable - SERC	
Answer	No
Document Name	
Comment	
Southern Company respectfully requests that the SDT refrain from attempting to define “communications networks” as an attempt could be defined so broadly to open the door to varying degrees of interpretation, or alternatively a restrictive definition could place limitations on a Responsible Entity’s implementation. The language, as specified in R1.2, places the responsibility on the Entity to define “the boundaries of *communication networks transmitting data* required for reliable operation” and should be determined by the Entity without the need for another defined term.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS recommended in its response to Question 8 that the term “communication networks” be replaced with the term “communication links.” AZPS recommends that the term “communication links” be defined as: The logical communication path that uses a routable protocol to connect BES Control Centers and over which Sensitive BES Data is transmitted. If the term “communication network” is retained, AZPS recommends the same definition: The logical communication path that uses a routable protocol to connect BES Control Centers and over which Sensitive BES Data is transmitted.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6	
Answer	No

Document Name	
Comment	
Tacoma supports the comments of Utility Services, Inc	
Likes 0	
Dislikes 0	
Response	
Charles Yeung - Southwest Power Pool, Inc. (RTO) - 2	
Answer	No
Document Name	
Comment	
The phrase “communication networks” is used elsewhere in the standards. To define the term for one standard would have unintended impacts on other standards.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gerry Adamski - Essential Power, LLC - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 1,3,5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
TVA suggests focusing on the “sensitive bulk electric system data” moving between Control Centers and not underlying communications infrastructure.	

Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 1,3,4,5,6	
Answer	Yes
Document Name	
Comment	
“A collection of interconnected components utilized for transmitting and/or receiving data.”	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy supports a definition of “communication networks”. Use of the term “communication” creates some ambiguity, particularly what types of communication this applies. It is not known if all forms of communication fall under this purview, specifically verbal communication avenues.	
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	

The collection of networked communication devices that provide routable transmission of data.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 3,5	
Answer	Yes
Document Name	
Comment	
Communication networks - Any technology that allows the transfer of information and data, including voice, between two endpoints.	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
NRG recommends that the SDT provide a defined term for “Communication Networks” into the the NERC GOT.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	

Comment
Texas RE would support the SDT in defining the term “communication networks”. In addition, Texas RE recommends adding the following to the list of examples of communication links: Data link(s) between a Generator Operators.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	

Comment
Proposed definition - Communication network is data link used to connect one location to another location for the purpose of transmitting and receiving digital data used in intra-Control Center communications for reliability operations of the BES.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	

Comment
IPC suggests communication networks be defined as, "Those networks used to logically and physically transport a communications link."

Likes 0	
Dislikes 0	

Response	
Aaron Austin - AEP - 3,5	
Answer	Yes
Document Name	
Comment	
AEP believes this will help define the extent of the requirements.	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 3,4	
Answer	Yes
Document Name	
Comment	
Proposed definition - Communication network is data link used to connect one location to another location for the purpose of transmitting and receiving digital data used in intra-Control Center communications for reliability operations of the BES.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT asserts that “networks” may be too broad and implicate unintended equipment based on a common understanding of the term. Consider the use of “Communication Link” instead. Proposed definition: communications infrastructure between two or more locations for the purpose of transmitting and receiving data.	

Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
A definition of “communication networks” should be provided in the context of the CIP standard. This would minimize the risk of miss interpretation by the entities. In this case, we think that part of the definition should mention the logical network, not the physical network (not the equipment). So the definition could be logical network that is being used to transport data used by the BES	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
We recommend the following definition: Communication Network: a system of sending and receiving information, i.e. data, from point A to point B using a network of logical and physical devices. The term ‘communication network’ excludes equipment facilities used exclusively for Interpersonal Communication or Alternative Interpersonal Communication, as defined in the NERC Glossary of Terms.	
Likes 3	PSEG - Public Service Electric and Gas Co., 1, Smith Joseph; PSEG - PSEG Fossil LLC, 5, Kucey Tim; PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Joe Tarantino - Sacramento Municipal Utility District - 1,3,4,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Yes – Clarity is always welcomed.	
Likes 0	
Dislikes 0	
Response	
Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
If the term “communication networks” is not formally defined, industry interpretations will vary widely.	
Likes 0	
Dislikes 0	
Response	
Candace Morakinyo - WEC Energy Group, Inc. - 3,4,5 - MRO,RF	
Answer	Yes
Document Name	
Comment	
The SDT needs to make it clear whether there are deliniations / transitions between routable and other forms (serial, dial-up) forms of communication network. They should also make it clear what specific protections apply to those parts of the communication network over which a Registered Entity has direct control (up to and including the ESP) and those parts over which a Registered Entity may have little or no control (e.g. network communication links between ESPs).	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 1,5	

Answer	Yes
Document Name	
Comment	
To promote consistency as the standards change, Reclamation recommends NERC define “communication network” in the NERC Glossary of Terms. Reclamation recommends the following definition of Communication Network: “A system of communication connections consisting of (but not limited to) cables, fibers, microwave radio links, satellites, etc. used to connect computers or other terminals for the purpose of exchanging data required for the reliable operation of the BES.”	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
See attachment Q1	
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	
We support a NERC Glossary Term for “Communication Network.” Suggested Definition	

Communication Network – Logical connections between two or more control centers which pass real time operational reliability data required for reliable operation of the Bulk Electric System. The connections may include, but are not limited to, physical equipment, through tunneling, or other virtual constructs. Potential GTB support: The Communication Network is a layer 3 (network layer) construct as established by the International Organization for Standardization (1989-11-15). "ISO/IEC 7498-4:1989 -- Information technology -- Open Systems Interconnection -- Basic Reference Model: Naming and	
Likes 0	
Dislikes 0	
Response	
sean erickson - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
The document continually uses the terms, “communication links”, “communication networks”, “data links”, “in-scope communication networks”, “in-scope communication links”, and in one case “communication networks/data links”, without clarifying the differences between any of the terms, or their intended use. This adds ambiguity to the document. Questions surface regarding the nature of a link being a single path, and do multiple links form a network? What is the difference between a communication link and a data link, does one carry voice traffic and the other does not? Do “in-scope” vs. “not in-scope” links or networks need to be identified separately? If the terms are being used interchangeably, then the correct term and its definition needs to be identified and used consistently.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	

Additional comments received by Chris Scanlon of Exelon

Questions

1. The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), perishable, and has a diminished need for protection over time. Do you agree with the SDT's assertion? If you agree, please supply a rationale to support the position.

☒ Yes
☐ No

Comments: Exelon agrees that the referenced data is already afforded protections at rest under the existing CIP Standards through physical and logical protections. The standards use a layered defense-in-depth approach based on the impact rating of the BES Cyber Systems. For example, for the BES Cyber Systems that communicate with a routable protocol using External Routable Connectivity, more granular security controls are applied to those BES Cyber Systems from CIP-005-5, CIP-006-6, CIP-007-6, and CIP-010-2. Whereas for those BES Cyber Systems that do not communicate externally, the CIP-006-6 standards affords specific physical security controls to "restrict physical access" along with the logical controls from CIP-007-6 and CIP-010-2 to support, malicious code prevention, security patch managements, configuration baselines, etc.

There is also a diminished need to protect real-time reliability operating data over time given that it is only used for real-time operation at a point-in-time. Once it is replaced by newer information, there is less of a need to protect the referenced data over time.

Additional thoughts & General Comments:

1) There is a disconnect between the requirement language and the Guidelines and Technical Basis (GT&B) section. The following examples identify specific instances where the GT&B and requirement language are inconsistent.

a. The draft requirement describes the applicable communication networks as those transmitting "data required for reliable operation of the BES" whereas the guidance refers to networks that transmit "operational reliability data between Control Centers." The former indicates a measure of Responsible Entity discretion in identifying the critical networks, whereas the latter would seem to capture any network transmitting operational reliability data, regardless of the effect of that data on reliable operation.

The guidance later refers to identifying "communication links that could adversely impact the reliable operation of the Control Center within 15 minutes." That seems to push for a measure of entity discretion in designing a process for identifying such networks and conflict with the identification of all networks that transmit "operational reliability data between Control Centers

b. The GT&B section uses wording such as "required" or "must" which is requirement language and not guidance. The GT&B is to explain the requirement language.

c. The GT&B states that "the Responsible Entity should ensure that the methods chosen include rationale supporting the identification of such communication networks" however the Requirement only states that there be "1.1 Procedure(s) to identify the communication networks requiring protections."

d. The GT&B suggests that a "Responsible Entity complement physical protections with logical protections to fully ensure that the integrity and confidentiality of data transmitted between Control Centers is protected." Are there cases where physical security would not be sufficient thereby making this a requirement to achieve the security objective.

e. The GT&B suggests that "the Responsible Entity must document and implement plans for the protection of the confidentiality and integrity of operational reliability data communicated between Control Centers." We are obligated to demonstrate that we have implemented the Plan(s), but this reads as if we have to have separate evidence that demonstrates the plans that were used to implement.

2) What does it mean for a communication network to be within an entity's "footprint"? Does that refer to networks within a retail distribution area? Does that refer to communication networks at an entity's facility? If it is associated with the" utility footprint", how does that concept apply to entities without a traditional utility "footprint" such as a GOP or RC?

3) The GT&B should specifically state that a Responsible Entity that lacks a Control Center is not subject to the Standard. For example, a GOP with only a control room for a single generating facility location would not have a "Control Center" and would not therefore be subject to the Standard. From a compliance perspective, it is helpful when the guidance says this explicitly.

4) By definition, only RCs, BAs, TOPs, and GOPs can have "Control Centers" yet the CIP Standards generally apply the DPs, TOs, GOs, and IAs as well. Are these latter entities exempt from the Standard?

5) The application of the Standard to protect communications networks should not inhibit an entity's ability to participate in programs (e.g. anti-terrorism, CRISP, etc.) where network connections to government or other entities are necessary to share information. The GT&B should provide guidance supporting that the protections of communications are not intended to inhibit these types of data monitoring activities or with the confidentiality and data integrity required by the Standard.

6) Addressing the need to clearly scope this Standard to ESP to ESP networks.

Below is discussion for allowing the Control Center to Control Center links assessed for this requirement in 1.1 to be able to be limited by a registered entity to Control Center ESP to Control Center ESP links (inter and intra). We would prefer to see the scope more defined within the Standard, but would at a minimum expect to see more clarity within the Guidance.

a. The guidance suggests the possibility of using NERC CIP-002 criteria to identify all inter-Control Center and intra-Control communication links. "As one possible solution, the Responsible Entity could apply CIP-002 criteria to identify all inter-Control Center and intra-Control

Center communication links that could adversely impact the reliable operation of the Control Center within 15 minutes." By application of the existing NERC CIP standards the CIP-002 criteria would identify communication links between ESPs (inter and intra Control Center).

There is an assumption statement that the SDT makes that is only true if the links are limited to ESP to ESP. "The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time. ". Non ESP devices holding operational data at rest may not be currently protected as part of NERC CIP standards as they are not in NERC CIP Scope. Example: PMU data transmitted between Control Centers but not having 15 minute impact.

b. Providing communications protections in this standard to non ESP to ESP links would mean that we are protecting networks under the rigor of this new NERC CIP standard without protecting the end devices (endpoints) under the NERC CIP requirements. By not using the same criteria there is risk to performers dealing with additional complexities of the NERC CIP standards and there is risk that auditors would initially interpret the end devices of these protected networks as being misclassified. The NERC CIP Standards determine the NERC CIP devices and the ESPs protecting those devices with a 15 minute impact criteria. The initial scope of the communications network requirements reasonably would be limited to links between those protected devices.

c. If planning and operational data without a 15 minute criterial is required to be in this standard then the standard needs more than network communications to ensure the standards cover that protection, it would require additional device protections.

d. With this allowed limitation of ESP to ESP links the issues related to a lack of clarity of "communication networks", "communication links", "sensitive bulk electric system data" are reduced as the scope of the protected networks is easily defined.

2. If you do not agree with the SDT's assertion in Question 1, please identify the type of data, the risk posed at rest, and supply the rationale to support the position.

   Comments:

   Not Applicable.

3. Future enforceable Reliability Standards IRO-010-2 and TOP-003-3 identify "data required for reliable operation." For example, Requirement R1 of IRO-010-2 states:

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include but not be limited to:

1.1. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Realtime Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator.

TOP-003-3 Requirements R1 & R2 also have similar requirements for BAs and TOPs.

Do you agree that outlining this approach for identifying "data required for reliable operation" in the Guidelines and Technical Basis is sufficient; consequently, an additional definition of "sensitive BES data" or a requirement to identify "sensitive BES data" is not necessary? If not, please explain.

☐ Yes
☐ No

Comments: Exelon does not agree with placing the obligation for what data is to be considered should be placed into the GT&B. Exelon does support leveraging existing descriptions of data required for reliable operation as much as possible so that data classified is consistent across the Standards. For entities covered by IRO-010 and TOP-003, CIP-012 should include in the Requirement language which data is required for protection. Having different groups of reliability data for the same entities will make compliance efforts needlessly complex with no added benefit to reliable operation.

4. The SDT asserts that "availability" of inter-and intra-entity Control Center communication of data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards, specifically Reliability Standards TOP-001-4 and IRO-002-5. The proposed standards require redundant and diversely routed data exchange capabilities at a Responsible Entity's primary Control Center. Do you agree that "availability" is adequately addressed by these standards? If not, please provide rationale to support your position.

☐ Yes
☐ No

Comments: Exelon agrees that the separate "Project 2016-01 Modifications to TOP and IRO Standards" covers the availability of the referenced data. In addition, covering the availability of data in this project goes beyond the scope of the Commission's directive, which is addressed only at protecting communication links and data for confidentiality and integrity.

5. The SDT is proposing to develop a new CIP standard because the directives of FERC Order 822 related to the protection of communication networks used to exchange sensitive BES data regardless of the entity's size or impact level. Do you agree with the drafting of a new CIP standard to address this issue? If you disagree and would prefer to include requirements in existing CIP Standards, such as CIP-003 and CIP-005, please provide rationale and propose requirement language.

☒ Yes
☐ No

Comments: Exelon agrees that the directive should be addressed through a new Standard, as proposed by the SDT. The other CIP Standards exempt "Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters." Revising those Standards to cover this new topic would require revisiting those exemptions in each Standard. It may be simpler to use an entirely specific Standard rather than re-opening the exemption for each existing CIP Standard.

6. The SDT evaluated multiple approaches to addressing the directive. The approach proposed in this informal posting focuses on the protection of communication links. An alternative approach could focus on the protection of the sensitive BES data itself. Do you agree with the SDT's approach to focus the draft language on the protection of communication links? If not, please provide rationale and propose alternative language.

☒ Yes
☐ No

Comments: Exelon supports responding to the directive by focusing on protecting the confidentiality and integrity of data sent over communication links; thereby applying protections to the data by addressing the communication links.

Exelon would prefer to change the "where technically feasible" language to "based on Cyber Asset capability." The version 5 set of Standards introduced the notion that there may be limitations to Cyber Assets and the SDT reduced the number of instances associated with Technical Feasibility Exceptions (TFE). For example, Requirement 1.3 could be rewritten to state: "Method(s) for protecting communication networks between Control Centers identified in 1.1, based on Cyber Asset **capability**." This would imply documenting the lack of capability but not require a TFE. Nearly any mitigating measures that would be required for a TFE could be considered protections that are documented to meet this requirement.

Exelon appreciates the SDT adding examples to the GT&B about approaches that can be implemented to meet the obligation of protecting communication networks. Exelon recommends that the SDT consider adding some text regarding the feasibility of these methods to the GT&B and whether the feasibility would ultimately affect whether the method would be viable:

- Site to site encryption – this is the most feasible approach at this time and focuses the protections on the end-points of the communications networks directly that make up the site-to-site encryption. Additionally, with this approach, there would not need to be an analysis of any of the intermediate communication networks or the transport layer communication networks since the site-to-site encryption protects the entire communication path.

- Application layer encryption – there are several barriers that would make this approach unlikely for mass use:
  - Lack of support – most vendors do not have these capabilities nor have them on their roadmaps
  - Lack of standards – if a vendor has application layer encryption it is most often proprietary
  - Lack of depth – some of the solutions that use SSL or TLS and all but TLS 1.2 have been deprecated.

  Once standards have been created for an interoperable application layer encryption protocol that also includes reliability and integrity features, then this would be the long range goal. This would provide the highest level of transport protections from device to device.
- Physical protections – depending on the size of the entity, deploying physical protections sufficient to protect the confidentiality and integrity of the referenced data, this may not be a feasible approach due to the cost of retrofitting and the limited protection it provides. It may be useful for short runs but as an overall approach may not possible.

7. Do you agree with the security objective of the draft language? If not, please propose alternative language.

   ☐ Yes
   ☐ No

   Comments: Exelon agrees with the security objective to protect communication networks between Control Centers. Exelon agrees with the security objective, however, requests the SDT add more clarity to the requirement language for what communication network end-points are actually expected to be protected and whether every intermediate communication network is required to be protected when implementations such as application-layer security or site-to-site virtual private networks are used.

8. Is it clear what types of plans, procedures, and methods are needed to meet the draft language? If not, please propose alternative language.

   ☐ Yes
   ☐ No

   Comments: The current draft language is reminiscent of V3 CIP-002 with entities determining their own risk based method without the guidance of a bright line. That did not work well to bring consistent implementation and left entities and regions unevenly protected. Defining the data to be protected as that which is transmitted between Control Center ESP to Control Center ESP (for High and Medium) does allow that bright line. If specific details related to the applicable protections are included in Guidance only, there will be

significant different interpretations. Exelon's preference would be to see more specificity within the Standard language itself. For entities without Electronic Security Perimeters, it is important to identify what end points need to be protected within the communication networks.

Implementation of Protections

1) Given proposed application to "inter-entity" communication networks, how will differences between entities be handled? For example:

a. If two entities take different approaches to encryption, how should that be resolved? Will there be dispute resolution of some kind?

b. What if one entity's approach is considerably more expensive and raises questions on prudency? How should that be resolved, particularly if utilities are in different states or have different rate structures that might not provide for the recovery of these costs?

c. If two entities have different opinions on whether their connecting communication network needs to be protected, whose view prevails?

i. Always the most conservative (protective) entity?

ii. Or is the Responsible Entity that identified the network as critical the only entity that needs to demonstrate compliance? If so, how can the other entity be required to undertake the costs necessary to assist the first entity in demonstrating compliance? (In other words, if I don't see a network as critical, why and how can I be required to spend money to assist you in implementing expensive encryption for purposes of your compliance?)

2) The guidance should expand on what is meant by "confidentiality" and "integrity" to ensure that auditors and Responsible Entities do not have different understandings of what the Standard is intended to accomplish.

- The reference to NIST Special Publication 800-53A is helpful, but it is not clear whether or not the Standard is specifically incorporating the definition of "integrity" contained in that publication. That publication also defines "confidentiality" but in a manner that includes personal data not relevant to NERC compliance.
- If the reference to NIST Special Publication 800-53A is intended to guide implication of the Standard in other ways, the guidance should explain how the NIST document is relevant. It appears to be focused on the assessment of confidentiality and integrity controls rather than the design of such controls.

3) The guidance states that physical conduit "can be used," but also suggests that conduit be supplemented by logical protections. Using conduit with additional logical controls might be a good security practice, but the Standard should specify that the use of physical conduit is sufficient to comply with the Standard. As written, it could be read that physical conduit, on its own, may not be sufficient for compliance.

4) Other than "site-to-site encryption" and "application layer encryption" are there other logical methods to protect data confidentiality and integrity that should be described in the program? The guidance does not limit Responsible Entities to those methods, but it can help from an audit perspective if the methods we use are described in the guidance.

9. The SDT uses the term "communication networks" throughout the draft language including an obligation to define the boundaries of such communication networks. Does the SDT need to define the term for inclusion in the NERC Glossary of Terms? If so, please propose a definition of "communication networks."

☐ Yes
☐ No

Comments: To ensure there is clear understanding of what communication networks are intended to be protected, the term "communication networks" should have a NERC defined definition. As written, the requirements and GT&B appear to commingle at what point of the "communication networks" are protections to be afforded. For example, the requirement "**1.1 Procedure(s) to identify the communication networks requiring protections**" obligation doesn't provide sufficient understanding of how to make that identification. Is the communication network that is local to the facility to be included, the communication network that is associated with the wide area network, or both. Moreover, requirement "**1.2 Procedure(s) for defining the boundaries of communication networks transmitting data required for reliable operation identified in 1.1, if applicable**" requires the entity to establish some boundary, but no clarity on how or what is an appropriate boundary. If an entity choses the boundary at the Electronic Security Perimeter to another Electronic Security Perimeter only, would that sufficiently addresses the security objective of the requirement?

The GT&B states that "The plan(s) should identify the applicable communication networks both within the entity's footprint, and any applicable networks between Responsible Entities." This statement adds additional ambiguity as to what points of the communication network are to be protected. If the Plan(s) are to take into account other networks "between Responsible Entities" does this also include the

telco provided networks? Depending on the solutions used, the intermediate communication networks are not a risk and are just the transport layer for the encrypted data packets.

Additional comments received from Vivian Vo of APS (Q8)

No, AZPS respectfully submits that the draft language is not clear relative to the types of plans, procedures, and methods that are needed for compliance therewith. In particular, AZPS has identified several revisions to the draft language that should be implemented to ensure clarity and consistency relative to the obligation being described:

- Evaluate and revise the introductory language to ensure that it is consistent with the content of the subparts;
- Replace the term "communication networks" with the term "communication links;" and
- Develop appropriate defined terms to ensure that the responsible entities have a clear and unambiguous scope and associated expectations and obligations (e.g., the term "communication networks" and the scope of data to which these requirements are applicable).

AZPS recommends these revisions as they will further ensure that the protections required by the FERC directive are clear and unambiguous and that protections are applied more uniformly across entities that communicate via the in-scope data links. Without such modifications, ambiguity coupled with the inherent complexity of the processes and data that are in-scope will create unnecessary risk and diminish the value and benefit of the protections implemented to the reliable operation of the BES.

AZPS recommends the following modifications to the draft language:

The Responsible Entity shall implement one or more documented plan(s) that ~~achieve the security objective to protect confidentiality and integrity of data required for reliable operation of the BES. The plan~~ applies to data being transferred across Communication ~~networks~~Links between Control Centers, both inter-entity and intra-entity, and that shall include each of the applicable parts below:

1.1 Procedure(s) to ~~identify the communication networks requiring protections~~ determine Sensitive BES Data transmitted between Control Centers requiring protections;

1.2 Procedure(s) for defining the boundaries of Communication ~~networks~~Links transmitting Sensitive BES Data ~~required for reliable operation identified~~determined in 1.1, if applicable;

1.3 Method(s) for protecting the confidentiality and integrity of data transmitted via these Communication ~~networks~~Links between Control Centers as ~~identified~~determined in 1.1, ~~where technically feasible.~~ via one or more of the following methods per Communication Link capability:

1.3.1 Encryption of the data prior to leaving the ESP or at the boundaries identified in 1.2, with decryption occurring at the boundary that the receiving Control Center has identified in 1.2.

1.3.2 Monitoring the status of the Communication Links and issuing an alarm or alert in response to detected communication failures or potential compromises to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.

1.3.3 Implementation of an equally effective logical protection.

Additional comments received from Nathan Mitchell of APPA

Questions

1. The SDT asserts that the referenced data is already afforded protections at rest under existing CIP standards (CIP-003, 005, 007, etc.), is perishable, and has a diminished need for protection over time. Do you agree with the SDT's assertion? If you agree, please supply a rationale to support the position.

   ☒ Yes

   ☐ No

   Comments:

   The referenced data while at rest is covered in the cited Standards. Consider that real-time SCADA data performance may be impacted by disk encryption.

2. If you do not agree with the SDT's assertion in Question 1, please identify the type of data, the risk posed at rest, and supply the rationale to support the position.

   Comments:

   No comment to this question

3. Future enforceable Reliability Standards IRO-010-2 and TOP-003-3 identify "data required for reliable operation." For example, Requirement R1 of IRO-010-2 states:

R1. The Reliability Coordinator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include but not be limited to:

1.2. A list of data and information needed by the Reliability Coordinator to support its Operational Planning Analyses, Real-time monitoring, and Realtime Assessments including non-BES data and external network data, as deemed necessary by the Reliability Coordinator.

TOP-003-3 Requirements R1 & R2 also have similar requirements for BAs and TOPs.

Do you agree that outlining this approach for identifying "data required for reliable operation" in the Guidelines and Technical Basis is sufficient; consequently, an additional definition of "sensitive BES data" or a requirement to identify "sensitive BES data" is not necessary? If not, please explain.

☒ Yes

☐ No

Comments:

We agree with the basic approach of using TOP-003 and IRO-010 Standards to identify this data but needs to be limited to real time data. We believe TOP-003 and IRO-010 include data that is not “real time” so would be outside this document’s scope. An example of data which is out of scope includes data used for Operational Planning Analyses.

4. The SDT asserts that “availability” of inter-and intra-entity Control Center communication of data is being addressed in Project 2016-01 Modifications to TOP and IRO Standards, specifically Reliability Standards TOP-001-4 and IRO-002-5. The proposed standards require redundant and diversely routed data exchange capabilities at a Responsible Entity’s primary Control Center. Do you agree that “availability” is adequately addressed by these standards? If not, please provide rationale to support your position.

☒ Yes

☐ No

Comments:

Availability is adequately covered by other standards.

5. The SDT is proposing to develop a new CIP standard because the directives of FERC Order 822 related to the protection of communication networks used to exchange sensitive BES data regardless of the entity’s size or impact level. Do you agree with the drafting of a new CIP standard to address this issue? If you disagree and would prefer to include requirements in existing CIP Standards, such as CIP-003 and CIP-005, please provide rationale and propose requirement language.

☒ Yes

☐ No

Comments:

There are concerns about the applicability section and how it will interact with the existing CIP Standards exemption 4.2.3.2. The

applicability section should limit the scope to only real time communication networks or data between Control Centers.

Would like additional guidance on the applicability of technologies like voice communication email, text messaging …

Consider including language for CIP Exceptional Circumstances

6. The SDT evaluated multiple approaches to addressing the directive. The approach proposed in this informal posting focuses on the protection of communication links. An alternative approach could focus on the protection of the sensitive BES data itself. Do you agree with the SDT's approach to focus the draft language on the protection of communication links? If not, please provide rationale and propose alternative language.

   ☐ Yes

   ☒ No

   Comments:

   We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. The Standard should be an outcome based Standard.

   FERC Order 822 section 58 clarifies this scope as inter-Control Center and intra-Control Center communications. The guidance seems to extend the scope beyond this by including references to DP's and listing Data links without reference to Control Centers.

7. Do you agree with the security objective of the draft language? If not, please propose alternative language.

   ☐ Yes

   ☒ No

   Comments:

   We suggest "reliability and availability" replace "confidentiality and integrity" because EMS/SCADA systems are built on "reliability and availability".

8. Is it clear what types of plans, procedures, and methods are needed to meet the draft language? If not, please propose alternative language.

   ☐ Yes

   ☒ No

   Comments:

We like the option to protect either the data or the links. We would like to see these options clearly defined within the requirements and not just in the guidance. Replace “communication networks” with “communication networks or BES reliability data”. Include in 1.1 that this is for networks or data between Control Centers.

9. The SDT uses the term “communication networks” throughout the draft language including an obligation to define the boundaries of such communication networks. Does the SDT need to define the term for inclusion in the NERC Glossary of Terms? If so, please propose a definition of “communication networks.”

☐ Yes

☒ No

Comments:

Recommend a NO vote on defining “communication network”

But consider that the FERC Order Section 58 clarifies the focus and the scope on inter-Control Center and intra-Control Center communications