

Consideration of Comments

Project Name:	2023-03 Internal Network Security Monitoring Draft 1 of CIP-015-1
Comment Period Start Date:	2/27/2024
Comment Period End Date:	3/18/2024
Associated Ballot(s):	2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 IN 1 ST Project 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan IN 1 OT

There were 73 sets of responses, including comments from approximately 160 different people from approximately 102 companies representing 7 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the [project page](#).

If you feel that your comment has been overlooked, let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, contact Vice President of Engineering and Standards, [Soo Jin Kim](#) (via email) or at (404) 446-9742.

Questions

1. [Based on industry comments, the DT unanimously voted to continue Project 2023-03 without the inclusion of EACMs, PACS, and PCA devices outside of the ESP. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.](#)

Summary Response:

Project 2023-03 – INSM received unanimous support for the Drafting Team’s (DT’s) decision to continue the project without the inclusion of EACM and PACS outside of the ESP in the scope of proposed Reliability Standard CIP-015-1.

2. [The Project 2023-03 DT decided to create a new objective-based standard \(CIP-015-1\) as opposed to revising one or more existing CIP Reliability Standards to ensure that the purpose and requirements are clear and allow for future expansion if necessary. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.](#)

Summary Response:

Project 2023-03 – INSM received overwhelming supported from industry to create a new objective-based standard (proposed Reliability Standard CIP-015-1) as opposed to revising Reliability Standard CIP-007-X with a new Requirement R6 and/or revising other existing CIP reliability standards.

3. [Based on industry feedback, the Project 2023-03 DT developed Requirement R1 of CIP-015-1 to address INSM within Responsible Entity’s ESP. Do you agree that proposed CIP-015-1 Requirement R1 is clear to that intent, and do you support this direction? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.](#)

Summary Response:

The Project 2023-03 DT appreciates the valuable feedback received regarding Question 3. To address the feedback received, the DT modified Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks

protected by the ESP that are the focus of Requirement R1, and 2) to ensure all requirement Parts are supported by the language in Requirement R1.

Additionally, the DT removed the words “increased the probability of” from Requirement R1. Moreover, recognizing that there are many approaches and methods to achieve the security objectives of this requirement, and that a “one-size-fits-all” approach might not align with all current and future network environments, the DT provided additional context in the Technical Rationale that can be leveraged to develop an INSM.

4. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.1 to allow Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks. The measures provide high-level guidance to achieving the risk-based approach. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The Project 2023-03 DT appreciates the valuable feedback received regarding Question 4. The DT made modifications to Requirement R1 Part 1.1. to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than alternative language proposed by several commenters. Moreover, the DT received comments that referenced “locations” could be confused with geographic locations, so the DT modified “network data locations and methods” with “network data feed(s)”.

The DT reviewed the SAR, and with respect to the reference to monitor network activity including software, it is the opinion of the DT that the network data related to software will be included in the elements contained in Requirement R1, Part 1.1.

5. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.2, which consolidated two requirement parts from the previous Draft to CIP-007-X, to have flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The use of the baseline is referenced in the measures as a method to demonstrate a method to meet the

[requirement part. Do you agree that the proposed CIP-015-1 Requirement R1, Part 1.2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.](#)

Summary Response:

The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was unnecessary to define the term in the NERC Glossary.

Anomalous - adjective

1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification

b: marked by incongruity or contradiction : PARADOXICAL

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

- 1.1.** Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.
- 1.2.** Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.
- 1.3.** Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

While CIP-007-6, Requirement R4, does allow logging of events at the BES Cyber System level, the DT determined that most entities are logging events at the Cyber Asset level in a security information and event management (SIEM) system. Additionally, the SIEM may be used for analysis and retention of those host-level events to meet CIP-007-6, Requirement R4 and allow for detection of login attempts and malicious code on those Cyber Assets.

The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

The DT agrees that striking “or unauthorized” in Requirement R1 better aligns with the other requirements in the proposed standard and updated Requirement R1 for Draft 2 of proposed Reliability Standard CIP-015-1.

6. Based on industry feedback, the Project 2023-03 DT has drafted language of Draft 1 of proposed CIP-015-1 Requirement R1, Part 1.3 for Registered Entities to have flexibility in order to evaluate activity detected in Part 1.2 to determine appropriate action. The measures provide high-level guidance to achieving the risk-based approach which may, or may not include, escalation of the CIP-008 Cyber Security Incident response plans. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective

1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification

b: marked by incongruity or contradiction : PARADOXICAL

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

- 1.1.** Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.
- 1.2.** Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.
- 1.3.** Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

The DT removed “appropriate action” and replaced it with “further action(s)”. Requirement 1, Part 1.3 was updated for Draft 2 to: “Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Network and metadata associated with anomalous network activity must be available for the evaluation conducted in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Network and other data associated with false positives and other detections deemed not to be malicious do not need to be further retained after the evaluation in Requirement R1, Part 1.3. However, data associated with potential attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity’s CIP-008 incident response process(es) for further investigation.

7. The Project 2023-03 DT has drafted Requirement R2 of proposed CIP-015-1 for Registered Entities to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification. Do you agree that the proposed CIP-015-1 Requirement R2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT has updated the Technical Rationale document for clarity on Requirement R2. Additionally, the DT has also created a FAQ document for this project that states, “Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.”

Requirement R2 has been revised to: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.”

The DT believes data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

Data protection in proposed Reliability Standard CIP-015-1, Requirement R2, is intended to protect the data from being altered or removed by an adversary intended to cover their tracks. BCSI protection as defined in the CMEP guide and CIP-011 is to protect against data or information that could be used to gain unauthorized access to a BES Cyber System.

8. The Project 2023-03 DT has drafted Requirement R3 of proposed CIP-015-1 for Registered Entities to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, which is the evaluation of anomalous activity in order to determine appropriate action. The goal of the Project 2023-03 DT was to allow Registered Entities to determine how to meet the objectives without defining strict duration that could cause the retention of substantial amounts of data that may not be relevant to meeting the security objects of the Reliability Standard. Do you agree that the proposed CIP-015-1 Requirement R3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT made the following changes:

- Requirement R3 was revised to the following:

“Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]”

- The DT added a note to R3 stating:

“Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.”

- The DT is hesitant to have potential overlap with an entity’s existing CIP-008 processes. The DT altered Requirement R1, Part 1.3 to state:

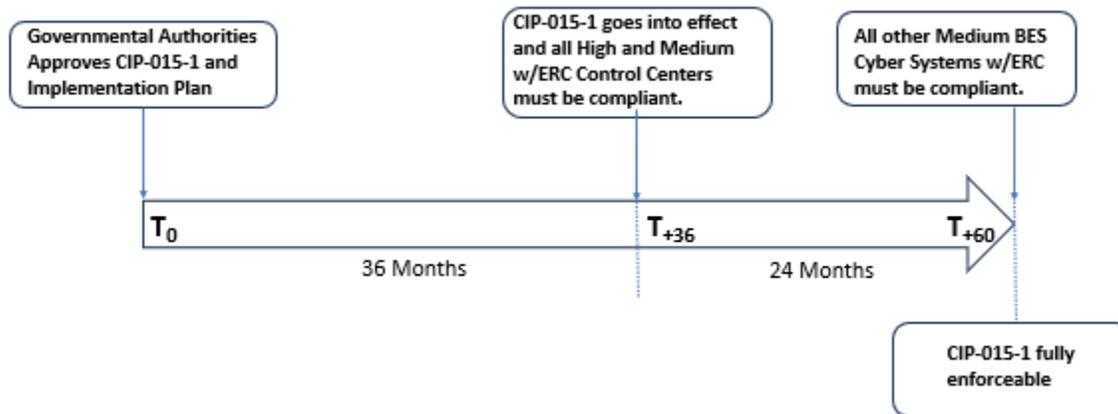
“Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine further action(s).”

The implication is that anomalous activity will require a response that could range from tuning software, if the activity is noise, to escalating into the CIP-008 process if it could potentially be a Cyber Security Incident or attempt to compromise.

9. Do you agree with the Implementation Plan for proposed CIP-015-1 that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations, which may be more challenging to implement.



10. Do you agree that the proposed CIP-015-1 is a cost-effective way to meet the reliability goal/FERC directives? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

FERC issued Order Nos. 893 and 893-A in 2023, which provide *Incentives for Advanced Cybersecurity Investment* as directed by the Infrastructure Investment and Jobs Act of 2021. The Order establishes rules for incentive-based rate treatment for certain voluntary cybersecurity investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the Order as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

11. Please provide any additional comments for the DT to consider, if desired.

Summary Response:

Generator Owners have been included in Section 4 Applicability. In a [letter order](#) issued on June 24, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," which officially effectuated NERC's transition away from the term "Special Protection System" to the newly-revised term "Remedial Action Scheme (RAS)."

The DT revised Requirement R1 and removed "or unauthorized" from the requirement.

For R1, the current draft has the language "Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications..." the DT believes that this will allow entities to customize their monitoring locations and to have a documented rationale for why those locations were chosen for audit defense.

The DT considered whether or not to create a NERC Glossary term for “anomalous.” After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective

1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification

b: marked by incongruity or contradiction : PARADOXICAL

Requirement R3 has been revised to the following:

“Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.”

The Standards Committee approved a waiver in August of 2023 that allowed the DT to post for as few as 20 days for industry comment. An additional waiver was approved by the Standards Committee in February 2024. These waivers were necessary to meet the regulatory deadline of July 2024.

The Industry Segments are:

- 1 — Transmission Owners
- 2 — RTOs, ISOs
- 3 — Load-serving Entities
- 4 — Transmission-dependent Utilities
- 5 — Electric Generators
- 6 — Electricity Brokers, Aggregators, and Marketers

- 7 — Large Electricity End Users
- 8 — Small Electricity End Users
- 9 — Federal, State, Provincial Regulatory or other Government Entities
- 10 — Regional Reliability Organizations, Regional Entities

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
					Adrian Andreoiu	BC Hydro and Power Authority	1	WECC
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Performance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Corporation (SPC)	1	MRO
					George Brown	Pattern Operators LP	5	MRO

					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities- Kansas (BPU)	1,3,5,6	MRO
					Peter Brown	Invenergy	5,6	MRO
					Angela Wheat	Southwestern Power Administration	1	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	TVA RBB	Ian Grant	Tennessee Valley Authority	3	SERC
					David Plumb	Tennessee Valley Authority	1	SERC
					Armando Rodriguez	Tennessee Valley Authority	6	SERC
					Nehtisha Rollis	Tennessee Valley Authority	5	SERC

Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	1	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
Jennie Wike	Jennie Wike		WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
Southern Company - Southern Company Services, Inc.	Jennifer Tidwell	1,3,5,6	SERC	Southern Company	Leslie Burke	Southern Company - Southern Company Generation	5	SERC
					Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC

					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
ACES Power Marketing	Jodirah Green	1,3,4,5,6	MRO,RF,SERC,Texas RE,WECC	ACES Collaborators	Bob Soloman	Hoosier Energy Electric Cooperative	1	RF
					Jennifer Bray	Arizona Electric Power Cooperative, Inc.	1	WECC
					Jason Proconiar	Buckeye Power, Inc.	4	RF
					Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Texas RE
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF

					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					Frank Lee	Pacific Gas and Electric Company	5	WECC
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	2	SERC
Black Hills Corporation	Rachel Schuldt	6			Micah Runner	Black Hills Corporation	1	WECC

				Black Hills Corporation - All Segments	Josh Combs	Black Hills Corporation	3	WECC
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
					Rachel Snead	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC

					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Gary Dollins	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Olivia Olson	Sho-Me Power Electric Cooperative	1	SERC

					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
					Heath Henry	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Brett Douglas	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Mark Riley	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Chuck Booth	Associated Electric Cooperative, Inc.	5	SERC
					Jarrold Murdaugh	Sho-Me Power Electric Cooperative	3	SERC

1. Based on industry comments, the DT unanimously voted to continue Project 2023-03 without the inclusion of EACMs, PACS, and PCA devices outside of the ESP. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer Yes

Document Name

Comment

Duke Energy supports this change, and thanks the Drafting Team for their careful consideration of the scope.

Likes 0

Dislikes 0

Response

Thank you for your support.

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer Yes

Document Name

Comment

PG&E supports the modifications.

Likes 0

Dislikes 0

Response

Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI comments: EEI agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
A PCA is within an ESP, the question is worded incorrectly.	
Likes	0
Dislikes	0
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	

Answer	Yes
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to MRO NSRF's comments.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
The term "PCA devices outside of the ESP" appears to contradict the NERC definition of PCA.	
Likes	0
Dislikes	0
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	

MRO NSRF supports this change, as the previous conditional inclusions were a source of confusion for many.

Likes 0

Dislikes 0

Response

Thank you for your support.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer Yes

Document Name

Comment

BPA endorses removing "EACMS, PACS, and PCA devices" from the requirements.

Likes 0

Dislikes 0

Response

Thank you for your support.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer Yes

Document Name

Comment

No additional comments

Likes 0

Dislikes	0
Response	
Thank you for your support.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company appreciates the change in scope for this version of the standard. The original scoping in the standard for individual systems outside of a defined ESP in requirements intended at a network (and not system) level is problematic. If the intent of the standard included system level monitoring rather than network monitoring only, how to scope such requirements to individual systems would be clearer. We appreciate the clearer scope.	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	
Supporting EEL comments for all questions	
Likes	0
Dislikes	0

Response	
Thank you for your support. Please see responses to EEI's comments.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Supporting EEI comments for all questions.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Richard Vendetti - NextEra Energy – 5	
Answer	Yes
Document Name	
Comment	
NEE support's EEI's comment(s): EEI agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
NST recommends that, for the sake of consistency with CIP-007, CIP-015's scope include BES Cyber Assets and any associated PCAs (which exist only inside ESPs).	
Likes	0
Dislikes	0
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes

Document Name	
Comment	
<p>WECC agrees with not including EACMS, PACS and PCAs outside ESP as it would not be consistent with the applicable systems scope of the SAR. However, we note that any scope of 'PCA devices outside of the ESP' is not supported by the definition of a PCA –</p> <p>'One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.'</p>	
Likes	0
Dislikes	0
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
With the caveat the PCAs by definition are inside an ESP and are in scope.	
Likes	0
Dislikes	0
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Clay Walker - Cleco Corporation - 1,3,5,6 – SERC	
Answer	Yes

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Teresa Krabe - Lower Colorado River Authority – 5	
Answer	Yes
Document Name	
Comment	
With the caveat the PCAs by definition are inside an ESP and are in scope.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

BHE agrees with the SDT’s decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.

Likes 0

Dislikes 0

Response

Thank you for your support.

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5

Answer Yes

Document Name

Comment

A PCA is within an ESP and the question is worded incorrectly

Likes 0

Dislikes 0

Response

Thank you for your support. The DT acknowledges the error of including PCA within Question 1.

Glen Farmer - Avista - Avista Corporation – 5

Answer Yes

Document Name

Comment

EEL agrees with the SDT’s decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.

Likes 0

Dislikes	0
Response	
Thank you for your support.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Alain Mukama - Hydro One Networks, Inc. – 1	
Answer	Yes
Document Name	
Comment	
Don't see the issue, but the final requirement verbiage should be clear on the Applicable System(s)/ESP.	
Likes	0
Dislikes	0
Response	
Thank you for your support. The DT acknowledges the error of including PCA within Question 1.	

Kinte Whitehead - Exelon – 3	
Answer	Yes
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI’s comments.	
Daniel Gacek - Exelon – 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI’s comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	

Comment

ITC supports EEI's comments on this project.

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI's comments.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer Yes

Document Name

Comment

OPG supports NPCC Regional Standards Committee's comments:

"A PCA is within an ESP and the question is worded incorrectly. "

Likes 0

Dislikes 0

Response

Thank you for your support. The DT acknowledges the error of including PCA within Question 1. Please see responses to NPCC RSC's comments.

Hillary Creurer - Allete - Minnesota Power, Inc. - 1

Answer Yes

Document Name

Comment

Minnesota Power supports EEI's comments.

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI's comments.

Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter

Answer Yes

Document Name

Comment

PCA devices do not sit outside of the ESP. Please clarify if the DT intention is to exclude PCA devices (in the ESP) or to simply exclude EACMS and PACS (outside of the ESP).

Likes 0

Dislikes 0

Response

Thank you for your support. The DT acknowledges the error of including PCA within Question 1.

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer Yes

Document Name

Comment

EEI agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
BHE agrees with the SDT's decision to continue Project 2023-03 without the inclusion of EACMS, PACS, and PCA devices outside of the ESP.	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	

Ruchi Shah - AES - AES Corporation – 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
James Keele - Entergy – 3	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Andrew Smith - APS - Arizona Public Service Co. - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC – 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Peter Yost - Con Ed - Consolidated Edison Co. of New York - 3	
Answer	
Document Name	
Comment	
SUPPORTING EEI COMMENTS ON ALL QUESTIONS.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

2. The Project 2023-03 DT decided to create a new objective-based standard (CIP-015-1) as opposed to revising one or more existing CIP Reliability Standards to ensure that the purpose and requirements are clear and allow for future expansion if necessary. Do you support this change? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer No

Document Name

Comment

SRP could support the creation of an entirely new standard once we understand the definition of “objective-based”. Please clarify “objective-based” or explain what it actually means.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT vetted the comment requesting clarification of “objective-based”. The DT believes the current revision of proposed Reliability Standard CIP-015 addresses this comment. The DT afforded entities’ flexibility in using various INSM methodologies and technologies, which are “objective-based”. Additionally, the DT updated the Technical Rationale document to reflect additional methods of analysis and to ensure that various tools can be used to comply with the newly drafted CIP-015 standard.

Alain Mukama - Hydro One Networks, Inc. – 1

Answer No

Document Name

Comment

If INSM not going to be in CIP-007 R6 and creating CIP-015 for INSM, why not move CIP-007 R4 Security Event Monitoring also to this new CIP-015?

Likes 0

Dislikes 0

Response

Thank you for your comment. The requirements of CIP-007, Requirement R4 applies to systems management, and CIP-015-1 applies to the network security monitoring.

Gail Golden - Entergy - Entergy Services, Inc. – 5

Answer No

Document Name

Comment

This creates a new standard in which creates a new monitoring standard when other standards already require monitoring (e.g CIP-003, CIP-005, CIP-007, CIP-010). Suggest consolidation of security monitoring standards.

Likes 0

Dislikes 0

Response

Thank you for your comment. At the start of Project 2023-03 INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on CIP-005 - Electronic Security Perimeter and CIP-007 – System Security Management. After careful consideration, the DT concluded that CIP-005 may not be suitable, as its primary focus is the establishment of the Electronic Security Perimeter (ESP) and the network communications into and out of the ESP. In addition, Project 2016-06 was making modifications to CIP-005 to align with zero trust approaches.

Regarding CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement 4 of CIP-007. However, after the initial posting and the subsequent feedback received, it became apparent that Standard CIP-007 may not align as well with our objectives.

CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated Electronic Access or Monitoring System (EAMCS), Physical Access Control System (PACS), and Protected Cyber Assets (PCA), which does not align perfectly with the scope of our Information Network Security Monitoring (INSM), as our focus lies on the data communicated within the networks containing BES Cyber Systems.

James Keele - Entergy – 3

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

This creates a new standard in which creates a new monitoring standard when other standards already require monitoring (e.g CIP-003, CIP-005, CIP-007, CIP-010). Suggest consolidation of security monitoring standards.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. At the start of Project 2023-03 INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on CIP-005 - Electronic Security Perimeter and CIP-007 – System Security Management. After careful consideration, the DT concluded that CIP-005 may not be suitable, as its primary focus is the establishment of the Electronic Security Perimeter (ESP) and the network communications into and out of the ESP. In addition, Project 2016-06 was making modifications to CIP-005 to align with zero trust approaches.

Regarding CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement 4 of CIP-007. However, after the initial posting and the subsequent feedback received, it became apparent that Standard CIP-007 may not align as well with our objectives. CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated Electronic Access or Monitoring System (EAMCS), Physical Access Control System (PACS), and Protected Cyber Assets (PCA), which does not align perfectly with the scope of our Information Network Security Monitoring (INSM), as our focus lies on the data communicated within the networks containing BES Cyber Systems.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp – 6

Answer	Yes
---------------	-----

Document Name	
Comment	
BHE agrees with the SDT’s decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT’s decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Hillary Creurer - Allete - Minnesota Power, Inc. – 1	
Answer	Yes/
Document Name	
Comment	

Minnesota Power supports EEI's comments.

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI's comments.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer Yes

Document Name

Comment

ITC supports EEI's comments on this project.

Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Daniel Gacek - Exelon – 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon – 3	
Answer	Yes
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes	0
Dislikes	0
Response	

Thank you for your support. Please see responses to EEI's comments.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	

Answer	Yes
Document Name	
Comment	
BHE agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	

Comment	
Ameren agrees with and supports EEI comments.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Richard Vendetti - NextEra Energy – 5	
Answer	Yes
Document Name	
Comment	
NEE support's EEI's comment(s): EEI agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	

While TVA understands the challenges to updating CIP-007 to include internal network security monitoring we believe that these changes should be included within existing monitoring requirements or those requirements, mainly CIP-007 R4, be moved to CIP-015 as well. INSM should be an extension of the existing required cybersecurity monitoring program, not a new program. By combining the two efforts some of the same requirements between CIP-007 R4 and the INSM components in CIP-015 may be used. Additionally, if the scope of the standard is expanded to Low systems in the future this will make it easier to apply the full monitoring program that would be needed.

Moving the proposed monitoring requirements to CIP-015 removes these obligations from the scope of the existing CIP-003 Cyber Security Policy – suggest consider revising CIP-003 to include CIP-015 in Cyber Security Policy.

Likes 0

Dislikes 0

Response

Thank you for your comment. The requirements of CIP-007, Requirement R4 applies to systems management, and proposed Reliability Standard CIP-015-1 applies to network security monitoring. At the start of Project 2023-03 INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on CIP-005 - Electronic Security Perimeter and CIP-007 – System Security Management. After careful consideration, the DT concluded that CIP-005 may not be suitable, as its primary focus is the establishment of the Electronic Security Perimeter (ESP) and the network communications into and out of the ESP. In addition, Project 2016-06 was making modifications to CIP-005 to align with zero trust approaches.

Regarding CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement 4 of CIP-007. However, after the initial posting and the subsequent feedback received, it became apparent that Standard CIP-007 may not align as well with our objectives. CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated Electronic Access or Monitoring System (EAMCS), Physical Access Control System (PACS), and Protected Cyber Assets (PCA), which does not align perfectly with the scope of our Information Network Security Monitoring (INSM), as our focus lies on the data communicated within the networks containing BES Cyber Systems.

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer Yes

Document Name

Comment

Southern Company agrees with the feedback by EEI.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI comments: EEI agrees with the SDT's decision to create a new objective-based Standard (CIP-015-1) instead of revising one or more existing CIP Reliability Standards.	

Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E supports the modifications.	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECl	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	

Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	

Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
TFIST had no comment on question 2	
Likes	0
Dislikes	0
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy supports this change and agrees that a new standard is the best approach to incorporating the INSM revisions.	
Likes	0
Dislikes	0
Response	
Thank you for your support.	

3. Based on industry feedback, the Project 2023-03 DT developed Requirement R1 of CIP-015-1 to address INSM within Responsible Entity’s ESP. Do you agree that proposed CIP-015-1 Requirement R1 is clear to that intent, and do you support this direction? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Ruchi Shah - AES - AES Corporation - 5

Answer No

Document Name

Comment

AES supports EEI comment below

EEI appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggest the following alternative language to reduce subjective language: “Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.”

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s Comments.

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer No

Document Name

Comment

Tri-State agrees with EEI comments below:

"EEI appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggest the following alternative language to reduce subjective language: “Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.”

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s Comments.

Wendy Kalidass - U.S. Bureau of Reclamation – 5

Answer

No

Document Name

Comment

Reclamation recommends there be more specific language on what risks should be identified or examples of what network security risks could exist.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. There are many approaches and methods to achieve the security objectives of this requirement and a “one-size-fits-all” approach might not align with all current and future network environments. The DT has provided additional context in the Technical Rationale that can be leveraged to develop an INSM and focusing on specific risks for the Responsible Entity.

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	No
Document Name	
Comment	
<p>Black Hills Corporation agrees with EEI’s comments: EEI appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggests the removal of “or unauthorized” from the requirement language to read as follows:</p> <p>Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of detecting anomalous (<i>remove: or unauthorized</i>) network activity. The documented process(es) shall include each of the applicable requirement parts.</p> <p>The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of “or unauthorized” clarifies the intention while meeting the security objective.</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI’s Comments.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	

The current requirement could be read that the network monitoring could be limited to High Impact and Medium Impact BCS. Suggest R1 be rewritten to state that the standard requires monitoring of the network within an ESP to include all systems that are connected therein, whether permanent or temporarily (such as Transient Cyber Asset).

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer No

Document Name

Comment

FirstEnergy believes clear separation of where CIP-005 ends and where CIP-015-1 begins in terms of enforcement would benefit the scope of CIP-015-1.

Since 'internal network security monitoring' will not be a defined term and Technical Rationale explanation are not part of the enforceable Requirement, FE asks the Drafting Team to more clearly identify their technical rationale in the standard so as to "help" Responsible Entities define that term for themselves, understanding the baseline knowledge of NERC and its Regional Entities.

Finally, FirstEnergy suggest removal of the conjunctive "or unauthorized" in the opening sentence of R1. The use of the term "unauthorized" hints at this should include some sort of authorization process paperchase for every network communication which is impractical and not related to potentially malicious network traffic.

Likes 0

Dislikes	0
Response	
<p>Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.</p>	
<p>Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</p>	
Answer	No
Document Name	
Comment	
<p>Southern Company agrees with the feedback by EEI. In addition, Southern has concerns with the phrase “increase the probability of detection” as the stated objective. Southern agrees that such a concept is necessary to prevent R1 from requiring 100% perfection of detection which no tool can guarantee. As this phrase is the core of the requirement's objective and what it is to accomplish, the focus is on an "increase" in probability and thus how your process accomplishes this increase, rather than whether the entity has implemented a process that can meet 1.1 to 1.3. A suggestion is to replace the phrase with “provide the capability of detection” or similar phrasing that is a far more binary judgment to make (did the entity implement a process to provide detection capability to meet all the requirement parts) and still avoids the 100% perfect detection of every anomaly issue. Therefore, if minimal change to R1 is required, we suggest the following (though we have a further suggestion of a more substantive change for consideration in Q4):</p> <p>Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability provide the capability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.</p>	
Likes	0
Dislikes	0
Response	

Thank you for your comment. Please see responses to EEI’s Comments.	
Richard Vendetti - NextEra Energy – 5	
Answer	No
Document Name	
Comment	
<p>NEE support’s EEI’s comment(s): EEI appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggests the removal of “or unauthorized” from the requirement language to read as follows:</p> <p>Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.</p> <p>The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of “or unauthorized” clarifies the intention while meeting the security objective.</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI’s Comments.	
David Jendras Sr - Ameren - Ameren Services – 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	

Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #3.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	No
Document Name	
Comment	

SMUD agrees with the comments submitted by Tacoma Power, and that the suggested language change to R1 is non-substantive and could be made for the final ballot posting.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to Tacoma Power’s comments.

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

Answer No

Document Name

Comment

Dominion Energy supports EEI comments

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s Comments.

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer No

Document Name

Comment

Project 2016-02 modified the concept of an EPS to include Zero-Trust architectures, where there is no “inside” or “outside” an ESP, but rather relies on the idea of “protected by an ESP.” Tacoma Power Suggests the following language for CIP-015 R1:

“Implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) or a medium impact BCS with External Routable Connectivity (ERC), **protected by an ESP**, to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]”

Tacoma Power thinks the language change to R1 is non-substantive and could be made for the final ballot posting.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC

Answer No

Document Name

Comment

Cleco agrees with EEI comments.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's Comments.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
<p>BHE appreciates the drafting team's revision to address INSM within the Responsible Entity's ESP through CIP-015-1 Requirement R1, but suggests the removal of "or unauthorized" from the requirement language to read as follows:</p> <p>Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity's ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.</p> <p>The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of "or unauthorized" clarifies the intention while meeting the security objective.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.</p>	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	

EEl appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggests the removal of “or unauthorized” from the requirement language to read as follows:

Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.

The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of “or unauthorized” clarifies the intention while meeting the security objective.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see the response to EEl's comments.

Robert Blackney - Edison International - Southern California Edison Company - 1

Answer No

Document Name

Comment

See comments submitted by the Edison Electric Institute.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEl’s Comments.

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	
Comment	
Clarity is required if INMS requirement is also applied to EACMS/PACS/PCA within ESP.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. There are many approaches and methods to achieve the security objectives of this requirement and a “one-size-fits-all” approach might not align with all current and future network environments. We provided additional context in the Technical Rationale that can be leveraged to develop an INSM.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI’s Comments.	
Daniel Gacek - Exelon - 1	
Answer	No

Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports EEI's comments on this project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's Comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	

OPG supports NPCC Regional Standards Committee’s comments:

"The current requirement could be read that the network monitoring could be limited to High Impact and Medium Impact BCS. NPCC RSC proposes to rewrite R1 to state that the standard requires monitoring of the network within an ESP."

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to NPCC RSC’s comments.

Hillary Creurer - Allele - Minnesota Power, Inc. - 1

Answer

No

Document Name

Comment

Minnesota Power supports EEI’s comments.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s Comments.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer

No

Document Name

Comment

SRP feels that there are no methods to measure compliance as the standard is stated. We ask to provide guidance as to what is required as evidence. Should detection be continuous, or is periodic detection permissible? Also, there is no timeline as to how often detection and evaluation should be performed (In real time? Every 15 minutes? Every 15 months?).

The standard does not make it clear of the word "baseline" is. Perhaps, the "definition" or the expectation of what the baseline is should be in the measures section. The technical rationale "definition" of a baseline is more clearly defined under Detection Methods "Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.". However, we did not see any reference to what is in the methods for this wording.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. Numerous comments were received expressing support for providing flexibility to Responsible Entities to develop their programs without having specific timelines and obligations that may not align to the operations of all Responsible Entities. We provided details in the Technical Rationale that can be used to support the INSM programs for the Responsible Entities. Additionally, the DT updated the Technical Rationale with additional language to clarify the word "baseline" when used to describe anomaly detection technology.

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECl

Answer No

Document Name

Comment

There is not a definition of "Network" in network security monitoring. While our *understanding* is that this standard is focused on network traffic monitoring, it is not explicit and, therefore, could be interpreted in multiple ways (EDR vs East/West traffic monitoring vs full network traffic monitoring, for example).

Likes 0

Dislikes	0
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
<p>EEI appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggests the removal of “or unauthorized” from the requirement language to read as follows:</p> <p>"Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of detecting anomalous network activity. The documented process(es) shall include each of the applicable requirement parts."</p> <p>The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of “or unauthorized” clarifies the intention while meeting the security objective.</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
<p>BHE appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggests the removal of “or unauthorized” from the requirement language to read as follows:</p> <p>Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.</p> <p>The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of “or unauthorized” clarifies the intention while meeting the security objective.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.</p>	
Bret Galbraith - Seminole Electric Cooperative, Inc. - 6	
Answer	No
Document Name	
Comment	

Seminole Agrees with the comments provided by EEI

"EEI appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggest the following alternative language to reduce subjective language: “Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.”

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s Comments.

Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6

Answer No

Document Name

Comment

Likes 0

Dislikes 0

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer Yes

Document Name

Comment

Duke Energy agrees that the parent requirement R1 of CIP-015-1 clearly addresses INSM within a Responsible Entity's ESP.

Likes 0

Dislikes 0

Response

Thank you for your support.

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer Yes

Document Name

Comment

PG&E agrees the modifications are clear on the intent and supports the modifications.

Likes 0

Dislikes 0

Response

Thank you for your support.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer Yes

Document Name

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum.

Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to MRO NSRF's comments.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF supports this clear direction.	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Existing monitoring standards are prescriptive to specific locations and event types that are possible to be monitored through traditional log review and automated evaluation. R1 is vague in the specific requirements that must be included in a process. Anomalous network activity is not defined within the standard or the glossary. This is left up to interpretation of the entity and the auditors. In the measures "Architecture documents" is beyond what is required for Electronic Security Perimeter drawings in CIP-005. Request for drawings should be limited to	

inclusions of elements within required drawings in the standards. The current draft of the standard also only allows for internal IDS types of solutions with detection event capturing and review.

Likes 0

Dislikes 0

Response

Thank you for your support. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The Measure was updated to remove the term “architecture” from the language. The Technical Rationale provides additional information to aid the Responsible Entity in developing their INSM program.

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE

Answer Yes

Document Name

Comment

PNMR agrees with intent of R1 but suggests changing the language from “to increase the probability of detecting” to “... to detect anomalous or unauthorized network activity”.

Likes 0

Dislikes 0

Response

Thank you for your support. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.

Based on the feedback the DT removed the words “increased the probability of” from Requirement R1.

Martin Sidor - NRG - NRG Energy, Inc. - 5,6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Anton Vu - Los Angeles Department of Water and Power - 6

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer Yes

Document Name

Comment

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
<p>Texas RE appreciates the drafting team’s efforts to be responsive to FERC Order No. 887. Texas RE is concerned, however, that the language in Requirement R1 does not lend to consistent application and would be a challenge to audit and enforce. Since the language in Requirement Part 1.1 does not establish a minimal level of acceptable monitoring or establish a maximum level of risk acceptance, an entity could determine that there are no network data collection locations and methods. If there are no network data collection locations and methods identified, Requirement Parts 1.2 and 1.3 would not be relevant.</p>	

Texas RE recommends clarifying “network security risk(s)”. The SDT could consider including network security risk criteria similar to how CIP-002 includes impact rating criteria or establishing minimum security risks similar to how CIP-007 Requirement R4 requires logging a minimum of certain types of events.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity; including connection, devices, and network communications. In addition, the associated measure states that the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected.

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5

Answer

Document Name

Comment

The current requirement could be read that the network monitoring could be limited to High Impact and Medium Impact BCS. TFIST proposes to rewrite R1 to state that the standard requires monitoring of the network within an ESP

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.

4. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.1 to allow Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks. The measures provide high-level guidance to achieving the risk-based approach. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Bret Galbraith - Seminole Electric Cooperative, Inc. - 6

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

Seminole agrees with comments from EEI

“EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.1 allows Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks, but suggests the following non-substantive revisions to the proposed language: “Identify network data collection location(s) and method(s), based on the network security risk(s), to monitor network activity including connection(s), devices, and network communications.” EEI proposes modifications to the draft M1, Part 1.1 measures to: “Architecture documents or other documents detailing data collection location(s) and method(s); or”

Seminole also agrees with Comments from Entergy

“ The requirement verbiage does not appear to be clearly aligned with expectations in the Measures and the Technical Rationale, which leads to audit risk for entities.

The wording of CIP-015-1 R1.1 requires entities to identify their network data collection locations and methods. This appears to provide entities the latitude to identify these points based on risk, but without an expectation of an exceedingly robust methodology and without an expectation to consider all possible network data collection locations. For example, an entity may decide to “collect all traffic from INSM from all ESP switches”, which would typically give large coverage of network traffic, but there may be additional network collection locations possible. However, the Measure (M1) for the requirement identifies an example of compliance evidence as “Documented rationale on how network locations were selected or excluded”, and the Technical Rationale “requires the Registered Entity to identify many possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cybersecurity monitoring purposes.”

If the intent is to require entities to develop a risk-based/ROI methodology to consider all/many network monitoring locations such that an entity cannot justify “collection of traffic from all network switches”, then the requirement should be updated to explicitly identify that expectation to start with a list of all/many locations and apply well defined risk-criteria and ROI criteria against that list to arrive at the final locations subject to the program, and all permutations of that list and criteria are subject to evidentiary review.”

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s comments and Entergy’s comments.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

BHE appreciates the drafting team’s revision to address INSM within the Responsible Entity’s ESP through CIP-015-1 Requirement R1, but suggests the removal of “or unauthorized” from the requirement language to read as follows:

Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of detecting anomalous or unauthorized network activity. The documented process(es) shall include each of the applicable requirement parts.

The proposed requirement language suggests that unauthorized network activity is a subset of anomalous network activity, and removal of “or unauthorized” clarifies the intention while meeting the security objective.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. To address commentor feedback, the DT made modifications to Requirement R1 to remove "or unauthorized" and made additional adjustments to the requirement to: 1) be clear it is the networks protected by the ESP that are the focus of Requirement R1, and 2) ensure all Requirement Parts are supported by the language in Requirement R1.

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer No

Document Name

Comment

EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language:

“Identify network data collection **point(s)** based on the network security **threat(s) and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications.”

These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity’s implementation of INSM.

We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language.

In addition, the DT received comments that referenced “locations” could be confused with geographic locations, and the DT modified “network data locations and methods” with “network data feed(s)”.

The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

FERC issued Order No. 893³ in 2023, which provides *Incentives for Advanced Cybersecurity Investment*. FERC Order No. 893 establishes rules for incentive-based rate treatment for certain voluntary cybersecurity investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the FERC Order No. 893 as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer

No

Document Name	
Comment	
<p>M1 1.1 - The term "documented rationale" is very open and can be a place where professional opinions may differ. A registered entity may have one an effective approach to monitoring but an auditor may have a differing opinion. While flexibility has its pro's and con's, some entities may prefer to have a little more specificity of what's needed to guide both the entity and regional entity audit staff.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the proposed alternative language. The Technical Rationale provides additional insights for Requirement R1, Part 1.1.</p>	
<p>Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez</p>	
Answer	No
Document Name	
Comment	
<p>No objectives to measure compliance have been provided. Self-proclaimed compliance would not be auditable (based on RE perception, rather than auditors). It is very vague, there is no measurement to consider what is acceptable. The entity can say I am always in compliance. There is no clear definition on how and how long to save off the data. Also, how to obtain the level of monitoring in the requirement is vague. This will be subjective vs objective. In addition, R1 1.1 states to identify location "based on the network security risk(s)" but does not attempt</p>	

to quantify specific risk or suggest which level of risk they're seeking to address. While entities can determine their own level of acceptable risk, this could lead to a wide range of outcomes.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. There are many approaches that can be taken to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.

Hillary Creurer - Allele - Minnesota Power, Inc. - 1

Answer No

Document Name

Comment

Minnesota Power supports EEI’s comments.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s comments.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer No

Document Name	
Comment	
<p>OPG supports NPCC Regional Standards Committee’s comments:</p> <p>"The current R1.1 requirements could be interpreted that a “Network Security Risk” evaluation or assessment could be required under the standard. NPCC RSC suggest removing “Network Security Risk” or stating that INSM should be for monitored of the entire network per technical capability or assets “Network Security Risk” for monitoring in a sub requirement(s). If a risk assessment is required, it should be stated in the standard clearly."</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. Please see responses to NPCC RSC’s comments.</p>	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
<p>ITC supports EEI’s comments on this project.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. Please see responses to EEI’s comments.</p>	
Daniel Gacek - Exelon - 1	
Answer	No

Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aligning with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	

See comments submitted by the Edison Electric Institute.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
<p>EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language:</p> <p>“Identify network data collection location(s) point(s) and method(s), based on the network security threat(s) risk(s) and technical capabilities identified by the Responsible Entity, to monitor network activity including connection(s), devices, and network communications.”</p> <p>These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity's implementation of INSM.</p> <p>We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.</p>	
Likes	0

Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
<p>BC Hydro appreciates the drafting team efforts and the opportunity to comment.</p> <p>The use of the 'risk-based' language in CIP-015 R1.1 is leaving it to the discretion of entities to determine which component poses higher or lower risks. This will leave it open to the auditor's interpretation and expectation instead of ensuring the scope is concise and clear under this requirement. BC Hydro recommends to define the parameters of these 'risks' to give clear direction to entities or specify the network components on which this requirement R1.1 applies.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. Many approaches can be taken to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.</p>	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No

Document Name	
Comment	
<p>BHE requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language:</p> <p>“Identify network data collection location(s) point(s) and method(s), based on the network security risk(s) identified by the Responsible Entity, to monitor network activity including connection(s), devices, and network communications.”</p> <p>We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. In addition, DT received comments that reference “locations” could be confused with geographic locations, and the DT modified “network data locations and methods” with “network data feed(s)”.</p> <p>The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.</p>	

FERC issued Order No. 893³ in 2023, which provides *Incentives for Advanced Cybersecurity Investment*. FERC Order No. 893 establishes rules for incentive-based rate treatment for certain voluntary cybersecurity investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the FERC Order No. 893 as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

Cleco agrees with EEI comments.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. Please see responses to EEI's comments.

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

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

Dominion Energy supports EEI comments

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. Please see responses to EEI's comments.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
<p>NST appreciates that the SDT has tried to avoid being overly prescriptive. However, we believe that instructing Entities to use a "risk-based approach" to designing and implementing INSM could result in endless arguments among Responsible Entities, Regions, and NERC over what might be considered acceptable risk-based approaches. We are even more concerned about the proposed criteria for Severe VSL for R1 ("The Responsible Entity did not identify network data collection locations and methods that provide value,..."). What is "provide value" intended to mean, and who would have the final say on whether a given Entity's INSM implementation was capable of doing so?</p> <p>NST recommends revising R1 Part 1.1 to simply state, "Identify network data collection locations and methods used to monitor network activity including connections, devices, and network communications."</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT received feedback that a provision is needed to allow for risk-based options. The Technical Rationale provides additional insights for Requirement R1, Part 1.1.</p>	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT joins the comments submitted by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to IRC SRC's comments.

David Jendras Sr - Ameren - Ameren Services - 3

Answer

No

Document Name

Comment

Ameren agrees with and supports EEI comments.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer

No

Document Name

Comment

The ISO/RTO Council (IRC) Standards Review Committee (SRC) is concerned that the Standard does not address scenarios in which no technical solution is available to achieve what the Standard requires, such as when an entity's environment includes devices that use non-standard

communication protocols. The SRC recommends that the standard be revised to address these types of scenarios, such as by allowing entities to apply for a Technical Feasibility Exception if circumstances warrant.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. The Technical Rationale provides additional insights for Requirement R1, Part 1.1. Furthermore, it is the DT’s opinion that a well-developed, risk-based rationale would avoid the need to file and maintain a Technical Feasibility Exception.

Richard Vendetti - NextEra Energy - 5

Answer No

Document Name

Comment

NEE is not in agreement with EEI’s comment

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT is unable to address your concern(s) since it is not indicated specifically what you disagree.

Andrew Smith - APS - Arizona Public Service Co. - 5

Answer No

Document Name	
Comment	
<p>AZPS agrees with EEI proposed revision to CIP-015-1 R1, Part 1.1:</p> <p>“Identify network data collection location(s) point(s) and method(s), based on the network security threat(s) risk(s) and technical capabilities identified by the Responsible Entity, to monitor network activity including connection(s), devices, and network communications.”</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. Please see responses to EEI’s comments.</p> <p>Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company</p>	
Answer	No
Document Name	
Comment	
<p>Southern agrees with and greatly appreciates the discussion in the TR on Part 1.1 and the degree of flexibility described there to “narrow the focus to collect the data that provides the highest benefit” and “narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data”. However, Southern suggests that R1 as worded implies a scope of 100% coverage of every subnet within in-scope ESPs. It is not until an example under the R1.1 measures that it mentions the potential exclusion of any network locations and the documentation of such.</p> <p>The TR states many different aspects to consider in choosing monitoring locations (value, benefit, cost-effectiveness, relevance, etc.) but R1.1 limits it to only network security risks. There is concern with the implication of “do all, but explain where you don’t” that this could require the documentation of network security risks for each IP subnet and “prove the negative” type evidence. As page 4 of the TR states network data collection location refers to both physical and logical networks, so there is concern with the large proliferation of logical networks with containerization (what used to be API calls are being replaced with virtual networks and IP addresses assigned to containers). Zero Trust principles and containerization call for ever more micro-segmentation and creation of virtual networks down to this level between</p>	

components of an application in a single system. As an example, documented reasons of why an entity did not monitor every internal virtual network generated by Docker between two components of a single application within a single Cyber Asset one could argue are of little value, but it seems would be necessary.

For all these reasons, we suggest a concept of a positive “identify where you do” rather than a sense of “explaining and documenting where you don’t”. The value of where to monitor is going to be based on the system’s architecture, especially in large, multi-layered, distributed systems. On the other end of the spectrum is a site that may have a router with an ACL on an ethernet port to an RTU, which is then connected serially to several relays. Monitoring that 2 node, single ethernet cable “internal network” ESP may be of no value as all traffic can be monitored on the other end of the circuit, and it is unclear whether the entity is compliant if they do so.

Southern suggests a concept for R1 and 1.1 such as:

R1. Responsible Entity shall implement one or more documented process(es) for Internal Network Security Monitoring (INSM) that includes:

R1.1 Identification of network data collection points by the Responsible Entity for its high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC).

We suggest that this covers monitoring the in-scope systems, but leaves flexibility on where such monitoring occurs on its networks and doesn’t imply “prove the negative” for every physical/virtual subnet that is not tapped and monitored.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language.

Robert Follini - Avista - Avista Corporation - 3

Answer

No

Document Name	
Comment	
<p>Avista agrees with comments by EEI (words in italics are requested to be struck)</p> <p>EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language:</p> <p>“Identify network data collection <i>location(s)</i> point(s) and <i>method(s)</i>, based on the network security threat(s) <i>risk(s)</i> and technical capabilities identified by the Responsible Entity, to monitor network activity including connection(s), devices, and network communications.”</p> <p>These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity’s implementation of INSM.</p> <p>We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI’s comments.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	

*“**R1.1** Identify network data collection locations and methods, **based on the network security risk(s)**, to monitor network activity including connections, devices, and network communications.”*

The bolded part ("based on the network security risk(s)") is not clear and can be open to interpretation of what is required. Therefore, it is recommended to require identification of the specific data collection locations and methods based on an entity's own experience and system needs.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. Many approaches can be utilized to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer No

Document Name

Comment

The “risk-based” language leaves it open for auditor interpretation. Meaning, auditors can determine that an entity did not apply the appropriate “risk-based” approach for their network security. BPA believes some level of deference must be offered to an entity’s risk management approach. Or, create auditor guidance on what a risk-based approach looks like with regards to INSM.

BPA reiterates its comments from the previous comment period regarding ‘risk-based approach’:

"BPA recognizes and appreciates the SDT's effort to allow Registered Entities (RE) to make their own risk-based determinations. BPA recommends that the current requirement language needs further refinement to clarify the intent. Ambiguity opens REs to subjective criticism from auditors... BPA suggests that R1.1 be rewritten to more clearly specify the requirement, such as "Use a risk-based assessment methodology to identify network data collection locations and methods..." Language used elsewhere in the CIP Standards, such as "as determined by the Registered Entity", could strengthen the position that the REs are empowered to set their own risk acceptance strategy, risk mitigation, etc."

BPA also asks the DT to clarify the term "locations" in the requirement, adding context currently only found in the Technical Rationale.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including "risk-based rationale" is more encompassing than the alternative proposed language. In addition, the DT received comments that referenced "locations" could be confused with geographic locations, and the DT modified "network data locations and methods" with "network data feed(s)".

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF

Answer	No
--------	----

Document Name	
---------------	--

Comment

The current R1.1 requirements could be interpreted that a "Network Security Risk" evaluation or assessment could be required under the standard. Cogentrix suggests removing "Network Security Risk" or stating that INSM should be for monitoring of the entire network per technical capability or assets "Network Security Risk" for monitoring in a sub requirement(s). If a risk assessment is required, it should be stated clearly in the standard. Furthermore, greater specificity should be offered for what 'network activity' entails. For connections,

monitored activity should include who, when, why, and how long; network communications should include type, port, bi-direction or unilateral, etc.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1.

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer

No

Document Name

Comment

The requirement verbiage does not appear to be clearly aligned with expectations in the Measures and the Technical Rationale, which leads to audit risk for entities.

The wording of CIP-015-1 R1.1 requires entities to identify their network data collection locations and methods. This appears to provide entities the latitude to identify these points based on risk, but without an expectation of an exceedingly robust methodology and without an expectation to consider *all* possible network data collection locations. For example, an entity may decide to “collect all traffic from INSM from all ESP switches”, which would typically give large coverage of network traffic, but there may be additional network collection locations possible. However, the Measure (M1) for the requirement identifies an example of compliance evidence as “Documented rationale on how network locations were selected or excluded”, and the Technical Rationale “requires the Registered Entity to identify many possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cybersecurity monitoring purposes.”

If the intent is to require entities to develop a risk-based/ROI methodology to consider all/many network monitoring locations such that an entity cannot justify “collection of traffic from all network switches”, then the requirement should be updated to explicitly identify that expectation to start with a list of all/many locations and apply well defined risk-criteria and ROI criteria against that list to arrive at the final locations subject to the program, and all permutations of that list and criteria are subject to evidentiary review.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than alternative proposed language. Many approaches exist that can be utilized to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer No

Document Name

Comment

Black Hills Corporation agrees with EEI’s comments: EEI requests the following revisions to the proposed CIP-015-1 Requirement R1, Part 1.1 language:

“Identify network data collection (*remove*: location(s)) **point(s)** (*remove*: and method(s)), based on the network security **threat(s)** (*remove*: risk(s)) **and technical capabilities identified by the Responsible Entity**, to monitor network activity including connection(s), devices, and network communications.”

These proposed revisions seek to clarify and offer additional flexibility for scenarios and environments where there are limitations on network connectivity and/or available bandwidth due to operational concerns that impact the entity’s implementation of INSM.

We also request the addition of examples and possible approaches to the implementation of INSM in environments where there are limitations on network connectivity and/or available bandwidth within the Technical Rationale and/or other appropriate supporting documentation.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s comments.

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

Answer

No

Document Name

Comment

Reclamation recommends there be more specific language on what risks should be identified or examples of what network security risks could exist.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. Many approaches exist that can be utilized to develop a risk-based

rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer No

Document Name

Comment

Duke Energy recommends the use of the word “points” instead of “locations” in R1.1.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. Moreover, the DT received comments that reference “locations” could be confused with geographic locations, and the DT modified “network data locations and methods” with “network data feed(s)”.

Ruchi Shah - AES - AES Corporation - 5

Answer No

Document Name

Comment

AES Support EEI comment below

EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.1 allows Registered Entities to identify network data collection location(s) and method(s) by implementing a risk-based approach focused on network security risks, but suggests the following non-substantive revisions to the proposed language: “Identify network data collection location(s) and method(s), based on the network security risk(s), to monitor network activity including connection(s), devices, and network communications.” EEI proposes modifications to the draft M1, Part 1.1 measures to: “Architecture documents or other documents detailing data collection location(s) and method(s); or”

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s comments.

Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6

Answer No

Document Name

Comment

Likes 0

Dislikes 0

Response

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer Yes

Document Name

Comment

While ACES agrees with the proposed language, in the past and near future, risk-based approaches NERC/FERC have not been happy with. Some good, Examples are CIP-002-3, CIP-014-1, CIP-013-1. With the above question #2 which contains “and allow for future expansion if necessary”, makes it appear that this proposed standard will be subject to change sooner than later, especially based on the changes proposed for CIP-014 and surely CIP-013-2 is next.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. Many approaches exist that can be utilized to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.

Colin Chilcoat - Invenergy LLC - 6

Answer Yes

Document Name

Comment

While Requirement R1, Part 1.1 is clear in intent, it must be supported by guidance on acceptable methods of monitoring network activity. For example, is monitoring activity at endpoints acceptable, or is dedicated monitoring equipment required? If a zero-trust strategy is implemented, can monitoring attempts to establish connections outside of the zero-trust architecture satisfy this requirement, or is a more traditional network intrusion detection solution required? It may not be practical to address such questions in the standard, but guidance documents that include technology options must reflect and support the intentions of the SDT.

Likes 0

Dislikes	0
Response	
Thank you for your comment. While end-point monitoring can be useful for an INSM program, the goal of the proposed Reliability Standard CIP-015-1 is monitoring network data feeds within the trusted zone.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Georgia System Operations Corporation supports ACES comments: "While ACES agrees with the proposed language, in the past and near future, risk-based approaches NERC/FERC have not been happy with. Some good, Examples are CIP-002-3, CIP-014-1, CIP-013-1. With the above question #2 which contains 'and allow for future expansion if necessary', makes it appear that this proposed standard will be subject to change sooner than later, especially based on the changes proposed for CIP-014 and surely CIP-013-2 is next."	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to ACES' comments.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
SPP respectfully asks the SDT to consider a "per system capability" clause due to potential technology limitations for entities (current and future technologies).	

Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language.</p>	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
<p>SMECO agrees with ACES comments:</p> <p>While ACES agrees with the proposed language, in the past and near future, risk-based approaches NERC/FERC have not been happy with. Some good, Examples are CIP-002-3, CIP-014-1, CIP-013-1. With the above question #2 which contains “and allow for future expansion if necessary”, makes it appear that this proposed standard will be subject to change sooner than later, especially based on the changes proposed for CIP-014 and surely CIP-013-2 is next.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. Please see responses to ACES’ comments.</p>	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	

Comment

CIP-015 R1.1 goes beyond the requirements in CIP-007. If we are logging events at a BES system level per the Cyber Asset capability then the network locations are already identified at the layer 2 and layer 3 devices within the scope of the existing cybersecurity monitoring program. By not updating existing monitoring standards the new standards are introducing additional complications to demonstrating how the monitoring program works overall. The statement based on network security risk(s) is vague on what risk should be evaluated or included in the assessment.

Likes 0

Dislikes 0

Response

Thank you for your comment. While end-point monitoring can be useful for an INSM program, the goal of proposed Reliability Standard CIP-015-1 is monitoring network data feeds within the trusted zone.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer Yes

Document Name

Comment

No additional comments

Likes 0

Dislikes 0

Response

Thank you for your support.

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer Yes

Document Name	
Comment	
PG&E agrees the modifications are clear on the intent.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster

Answer Yes

Document Name

Comment

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
The current R1.1 requirements could be interpreted that a “Network Security Risk” evaluation or assessment could be required under the standard. TFIST suggest removing “Network Security Risk” or stating that INSM should be for monitored of the entire network per technical capability or assets “Network Security Risk” for monitoring in a sub requirement(s). If a risk assessment is required, it should be stated in the standard clearly.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. Many approaches exist that can be utilized to develop a risk-based	

rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE is concerned the enforceable language of the requirement does not specify that the Responsible Entity is required to document the rational/justification for inclusion or exclusion of data collection location(s) and method(s) based on a risk-based approach in determining what data is necessary to monitor network activity. The SDT should consider requiring entities to justify the parameters they have developed to meet the requirement.

The SAR for this project states, “Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, network communications, and software inside the CIP-networked environment.” Texas RE noticed that software inside the CIP-networked environment is omitted from the requirement language. If the SDT intentionally omitted this language, then no change is needed. If the SDT did not intend to omit the language, Texas RE recommends including software in the requirement language.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. Many approaches exist that can be utilized to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this

Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale. Moreover, the DT reviewed the SAR, and with respect to the reference to monitor network activity including software, the opinion of the DT is the network data related to software will be included in the elements contained in Requirement R1, Part 1.1.

James Keele - Entergy - 3

Answer

Document Name

Comment

The requirement verbiage does not appear to be clearly aligned with expectations in the Measures and the Technical Rationale, which leads to audit risk for entities.

The wording of CIP-015-1 R1.1 requires entities to identify their network data collection locations and methods. This appears to provide entities the latitude to identify these points based on risk, but without an expectation of an exceedingly robust methodology and without an expectation to consider **all** possible network data collection locations. For example, an entity may decide to “collect all traffic from INSM from all ESP switches”, which would typically give large coverage of network traffic, but there may be additional network collection locations possible. However, the Measure (M1) for the requirement identifies an example of compliance evidence as “Documented rationale on how network locations were selected or excluded”, and the Technical Rationale “requires the Registered Entity to identify many possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cybersecurity monitoring purposes.”

If the intent is to require entities to develop a risk-based/ROI methodology to consider all/many network monitoring locations such that an entity cannot justify “collection of traffic from all network switches”, then the requirement should be updated to explicitly identify that expectation to start with a list of all/many locations and apply well defined risk-criteria and ROI criteria against that list to arrive at the final locations subject to the program, and all permutations of that list and criteria are subject to evidentiary review.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Project 2023-03 DT appreciates the valuable feedback received regarding this question. The DT made modifications to Requirement R1, Part 1.1 to implement, using a risk-based rationale, network data feeds to monitor network activity (including connection, devices, and network communications). In addition, using the associated Measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected. The DT believes that including “risk-based rationale” is more encompassing than the alternative proposed language. Many approaches exist that can be utilized to develop a risk-based rationale, and the DT does not want to limit options for Responsible Entities. The Technical Rationale provides additional insights for this Requirement R1, Part 1.1 and can aid in the development of the risk-based rationale.

5. Based on industry feedback, the Project 2023-03 DT has drafted proposed CIP-015-1 Requirement R1, Part 1.2, which consolidated two requirement parts from the previous Draft to CIP-007-X, to have flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The use of the baseline is referenced in the measures as a method to demonstrate a method to meet the requirement part. Do you agree that the proposed CIP-015-1 Requirement R1, Part 1.2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Ruchi Shah - AES - AES Corporation - 5

Answer No

Document Name

Comment

AEs Supports EEI comment below

EEI appreciates the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed. The description of of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”

As described in the response to question 3, R1 uses the terminology “anomalous or unauthorized network activity” but Requirement Part 1.2 uses the term “anomalous network activity” and Part 1.3 uses the term “activity detected” with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
<p>Tri-State agrees with EEI comments below:</p> <p>"The description of of the term "baseline" in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that "[m]any vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not."</p> <p>"As described in the response to question 3, R1 uses the terminology "anomalous or unauthorized network activity" but Requirement Part 1.2 uses the term "anomalous network activity" and Part 1.3 uses the term "activity detected" with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope."</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	

If the term “anomalous” is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. If entities are allowed the latitude to define criteria for anomalous events to report to in CIP-008, they should be afforded that opportunity for anomalous events in this standard. The Technical Rationale does provide additional detail regarding “anomalous” and the types of tools/methods that can help meet this standard, but without a clear definition of expectations from NERC, or the explicit ability for entities to define their “anomalous” criteria and monitoring program, compliance evaluation ambiguity still exists for entities both internally and externally.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was unnecessary to define the term in the NERC Glossary.

Anomalous - adjective

1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification

b: marked by incongruity or contradiction : PARADOXICAL¹

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

¹ <https://www.merriam-webster.com/dictionary/anomalous>

- 1.4. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.
- 1.5. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.
- 1.6. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer	No
Document Name	
Comment	
<p>If the term “anomalous” is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. If entities are allowed the latitude to define criteria for anomalous events to report to in CIP-008, they should be afforded that opportunity for anomalous events in this standard. The Technical Rationale does provide additional detail regarding “anomalous” and the types of tools/methods that can help meet this standard, but without a clear definition of expectations from NERC, or the explicit ability for entities to define their “anomalous” criteria and monitoring program, compliance evaluation ambiguity still exists for entities both internally and externally.</p>	
Likes	0
Dislikes	0

Response

Thank you for your comment. The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was unnecessary to define the term in the NERC Glossary.

Anomalous - adjective
 1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification

b: marked by incongruity or contradiction : PARADOXICAL²

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

- 1.1.** Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.
- 1.2.** Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.
- 1.3.** Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF

Answer	No
Document Name	
Comment	

The implementation of the INSM (1.2 and 1.3) should be a separate requirement. The standard should explicitly say a baseline is required or not required. The standards are ambiguous on if a baseline is required in its current version. However, It is clear that detection of anomalous activity has to be referenced to some standard/metric so it would appear that a baseline would be required, and as such should be stated explicitly.

Further, this approach appears inconsistent with existing requirements in CIP-007, R4, which calls for generation of alerts for security events. Should not this capability exist for ISNM as well that could then be evaluated in R1.3?

² <https://www.merriam-webster.com/dictionary/anomalous>

Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.</p> <ul style="list-style-type: none"> 1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications. 1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1. 1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s). <p>While CIP-007-6, Requirement R4, does allow logging of events at the BES Cyber System level, the DT believes that most entities are logging events at the Cyber Asset level in a security information and event management (SIEM) system. Additionally, the SIEM may be used for analysis and retention of those host-level events to meet CIP-007-6, Requirement R4 and allow for detection of login attempts and malicious code on those Cyber Assets.</p>	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
<p>NST disagrees with the SDT's decision to demote network baselining from a Requirement to a Measure, which is essentially nothing more than a suggestion, for two reasons:</p> <p>> FERC Order 887 Paragraph 5 states explicitly, "First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment."</p>	

> We are hard-pressed to imagine how anyone using INSM could detect anomalous network behavior without a baseline. To that point, Order 887 Paragraph 12 states, "Establishing baseline network traffic allows entities to define what is and is not normal and expected network activity and determine whether observed anomalous activity warrants further investigation."

Likes 0

Dislikes 0

Response

Thank you for your comment. Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer

No

Document Name

Comment

Tacoma Power supports the EEI comments for consistency of language on what to detect (i.e. anomalous or unauthorized). Tacoma Power thinks the language change to Part 1.2 is non-substantive and could be made for the final ballot posting.

Likes 0

Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
<p>OPG supports NPCC Regional Standards Committee's comments:</p> <p>"The implementation of the INSM (1.2 and 1.3) should be a separate requirement. The standard should explicitly say a baseline is required or not required. The standards are ambiguous on if a baseline is required in its current version."</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to NPCC RSC's comments.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	No
Document Name	
Comment	
<p>Part 1.2 refers to "data collected at locations identified in Part 1.1," but it seems that depending on the method used to collect and identify anomalous information, the data collection location may not be relevant. Suggested language: "Implement one or more method(s) to detect anomalous network activity using the data collected pursuant to Part 1.1."</p>	
Likes	0

Dislikes	0
Response	
Thank you for your comment. The DT updated Requirement R1, Parts 1.1., 1.2., and 1.3 for clarity.	
<ul style="list-style-type: none"> 1.4. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications. 1.5. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1. 1.6. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s). 	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
<p>This would require knowledge of previous context and in order to be compliant, it appears that a baseline would be required to compare network activity to detect “anomalous” activity. SRP strongly feels that it should be stated specifically in the standard. Also, as previously stated, the requirement is still not clear of the word "baseline" and perhaps a definition or explanation should be included in the measurements section. SRP also suggest that in the Methods it includes what the Technical rational has defined as a "baseline" as the word "baseline" is still confusing since the baseline is also used in CIP-010 R1.</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.	

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

Bret Galbraith - Seminole Electric Cooperative, Inc. - 6

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

Seminole supports the comments from EEI

“The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. Please see responses to EEI’s comments.

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment

Duke Energy agrees that Part 1.2 is clear and an objective-based approach that requires one of more methods to detect anomalous network activity without the prescriptive requirement of a baseline.

Likes 0

Dislikes 0

Response

Thank you for your support.

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer Yes

Document Name

Comment

PG&E agrees the modifications are clear on the intent.

Likes 0

Dislikes 0

Response

Thank you for your support.

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer Yes

Document Name

Comment

Black Hills Corporation agrees with EEI’s comments: EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.

The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. Please see responses to EEI’s comments.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	Yes
--------	-----

Document Name	
---------------	--

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your support. Please see responses to MRO NSRF’s comments.

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	Yes
--------	-----

Document Name	
Comment	
MRO NSRF appreciates and endorses this approach, which is clear in its intent. However, there is a concern that the phrase “detecting anomalous or unauthorized network activity” in R1 does not align well with Parts 1.2 and 1.3. We recommend striking “or unauthorized” in R1 to better align with the rest of the standard. As unauthorized network activity would also be anomalous, nothing would be lost with its omission.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT agrees that striking “or unauthorized” in Requirement R1 better aligns with the other requirements in the proposed standard and updated Requirement R1 for Draft 2.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA endorses removing "baseline" language from the requirement.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes

Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern agrees with the feedback by EEI. In addition, we do note the wording in the 1.2 requirement part is “anomalous”, but the measure switches to “unauthorized”. Per our comment on R1, we would suggest this be changed in the measure to match the requirement. A baseline of normal traffic could be used to show what is anomalous but would not determine what is unauthorized.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments. The DT updated the Measures to align with the revisions in Draft 2 of proposed Reliability Standard CIP-015-1.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	

Comment

Including measures referencing documentation of a network baseline not included in the standard does not make it an obligation of the requirement. Suggest remove from the measures. Instead, suggest the standard list specific events that an entity should be looking for as a minimum requirement.

Likes 0

Dislikes 0

Response

Thank you for your support. The DT updated the Requirements, Requirement Parts, and Measures to align with the revisions in Draft 2 of proposed Reliability Standard CIP-015-1.

Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE

Answer Yes

Document Name

Comment

PNMR agrees with the SDT to remove the term “baseline” from the requirement language. It does, however, believe that the term “baseline” in the Technical Rationale should be replaced with “expected network behavior”.

Likes 0

Dislikes 0

Response

Thank you for your support. The DT updated the Technical Rationale document to include a parenthetical after the word “baseline” “(expected network behavior).”

Richard Vendetti - NextEra Energy - 5

Answer Yes

Document Name

Comment

NEE support’s EEI’s comment(s): EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.

The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI’s comments.

David Jendras Sr - Ameren - Ameren Services - 3

Answer	Yes
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

BHE agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.

Likes 0

Dislikes 0

Response

Thank you for your support.

Glen Farmer - Avista - Avista Corporation - 5

Answer Yes

Document Name

Comment

EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.

The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”

Likes 0

Dislikes 0

Response

Thank you for your support.

Robert Blackney - Edison International - Southern California Edison Company - 1

Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	

Exelon supports the comments submitted by the EEI for this question.

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI's comments.

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer Yes

Document Name

Comment

ITC supports EEI's comments on this project.

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI's comments.

Hillary Creurer - Allete - Minnesota Power, Inc. - 1

Answer Yes

Document Name

Comment

Minnesota Power supports EEI's comments.

Likes 0

Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECl	
Answer	Yes
Document Name	
Comment	
<p>M1 1.2 -The phrase "Documentation of baseline used" does not adequately capture how these tools work. Some entities configure settings of these tools to only alert on exceptions to a baseline, but it's not like the software baseline that is easily discernable. Explicit baselines may be problematic since the tools are typically based on learning to detect anomalies, though feels our approach would be to provide the configuration settings used for the monitoring tool. This is more of a compliance concern as some entities may leverage other options to demonstrate compliance than a baseline.</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. The DT updated Measure 1, Part 1.2 for Draft 2 of proposed Reliability Standard CIP-015-1:	
<ul style="list-style-type: none"> Documentation detailing network data feed(s) that includes a documented risk-based rationale that describes how network data feed(s) were selected for data collection. 	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

EEI agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.

The description of the term “baseline” in the draft Technical Rationale clarifies the intention of Requirement R1, Part 1.2. Page 10 of the draft Technical Rationale explains that “[m]any vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.”

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your support.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
--------	-----

Document Name	
---------------	--

Comment

BHE agrees with the revisions made by the SDT to enable flexibility in approaches to identify anomalous activity without prescribing that a baseline be developed.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your support.

Martin Sidor - NRG - NRG Energy, Inc. - 5,6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	

Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Amy Wilke - American Transmission Company, LLC - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE is concerned with the removal of explicit requirements such as baselining to accomplish the security objective of implementing methods to detect anomalous network traffic. FERC Order No. 887 recognizes that establishing baselines is the primary means to identify anomalous traffic within an entities’ CIP-network environment, noting that “any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment.” FERC Order No. 887, at ¶ 79. Texas RE notes that FERC Order No. 887 does contemplate that the final rule should “provide flexibility to responsible entities in determining the best way to identify anomalous activity to a high-level of confidence, so long as the methods ensure: (1) logging of network traffic . . . (2) maintaining those logs, and other data collected, regarding network traffic that are of sufficient data fidelity to draw meaningful conclusions and support incident investigation, and (3) maintaining the integrity of those logs and other data by implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures . . . FERC Order No. 887, at ¶ 80.

While recognizing this need for flexibility, however, Texas RE is concerned that some of the identified measures, such as a list of detection events or INSM configuration settings, may be too vague to provide meaningful evidence that the detection of anomalous network activity security objective is being meaningfully performed. To prevent this, Texas RE suggests inserting language in the measures that clarify that, at a minimum, data collection methods must be of sufficient data fidelity to draw meaningful conclusions and support incident investigation consistent with the language in FERC Order No. 887.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT updated the Requirements, Requirement Parts, and Measures to align with the revisions in Draft 2 of proposed Reliability Standard CIP-015-1.

Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5

Answer

Document Name

Comment

The implementation of the INSM (1.2 and 1.3) should be a separate requirement. The standard should explicitly say a baseline is required or not required. The standards is ambiguous on if a baseline is required in its current version.

Likes 0

Dislikes 0

Response

Thank you for your comment. Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

6. Based on industry feedback, the Project 2023-03 DT has drafted language of Draft 1 of proposed CIP-015-1 Requirement R1, Part 1.3 for Registered Entities to have flexibility in order to evaluate activity detected in Part 1.2 to determine appropriate action. The measures provide high-level guidance to achieving the risk-based approach which may, or may not include, escalation of the CIP-008 Cyber Security Incident response plans. Do you agree that proposed CIP-015-1 Requirement R1, Part 1.3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer No

Document Name

Comment

A clear definition of “anomalous” is needed in order to determine compliance. For example, in Generation, certain activity that may take place during an outage may not be considered “anomalous” and would not invoke CIP-008. Also, the wording "Registered Entities to have flexibility in order to evaluate activity detected in Part 1.2 to determine appropriate action." is of a concern. It is vague and lets entities make their own decisions, which could be seen as audit bait when being audited.

Likes 0

Dislikes 0

Response

Thank you for your comment.

The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective

1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification
 b: marked by incongruity or contradiction : PARADOXICAL³

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

- 1.7. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.
- 1.8. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.
- 1.9. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	
Comment	
<p>BC Hydro has concerns in relation to the use of term "anomalous activity" as this could be varied in terms of application and usage and is left to the entities to interpret.</p> <p>BC Hydro also has concerns over the expected evidence needed for "documentation of responses to detected anomalies" per Measure M1 to meet Part R1.3., which seems to indicate that proof that all detections were responded to regardless whether they were false positives will be required, i.e. proving the negative on all anomalies detected. Due to this BC Hydro has concerns over a very high amount of data which needs to be analyzed and documented based on Requirement R1 Part R1.3 as drafted.</p>	

³ <https://www.merriam-webster.com/dictionary/anomalous>

BC Hydro recommends to make the scope concise in the language of CIP-015 Requirement R1 Part R1.3, and add example scenarios and use-cases in the Technical Rationale.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was unnecessary to define the term in the NERC Glossary.

Anomalous - adjective

1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification

b: marked by incongruity or contradiction : PARADOXICAL⁴

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

1.10. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.11. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.12. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

⁴ <https://www.merriam-webster.com/dictionary/anomalous>

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No, NCPA agrees with EEI comments about the word "appropriate" being too open for interpretation.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
Tri-State agrees with EEI comments below:	
"The term "appropriate" is a subjective term. We propose the following revision: "Implement one or more method(s) to respond to anomalous network activity detected in Part 1.2" This language is similar to the language used in CIP-008-6.	
Additionally, as described in the response to question 3, R1 uses the terminology "anomalous or unauthorized network activity" but Requirement Part 1.2 uses the term "anomalous network activity" and Part 1.3 uses the term "activity detected" with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope."	
Likes	0
Dislikes	0

Response	
Thank you for your comment. Please see responses to EEI's comments.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
<p>Duke Energy believes that the “appropriate action” language is too subjective and should be removed. We understand that in the process of tuning INSM implementations may generate lots of alerts, with the majority being false positives. We think that there is a way to tie the language to CIP-008 without arbitrarily treating each alert as an attempt to compromise. We suggest “Implement one or more method(s) to evaluate activity detected in Part 1.2 to determine if a CIP-008 Cyber Security Incident response plan activation is required as a response.</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. The DT removed “appropriate action” and replaced it with “further action(s)”. Requirement 1, Part 1.3. was updated for Draft 2 to, “Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).”	
Ruchi Shah - AES - AES Corporation - 5	
Answer	No
Document Name	
Comment	
<p>AES agrees that Part R1.3 provides entities the flexibility to evaluate and determine appropriate action. However, from the point where a determination is made and going forward, all related activities should be driven by existing Requirements in CIP-008.</p>	

AES also agrees with EEI comment below

EEI appreciates the SDT’s revisions to allow Registered Entities to have flexibility to evaluate activity detected in Part 1.2 to determine appropriate action, however, the term “appropriate” is a subjective term. We propose the following revision: “Implement one or more method(s) to respond to anomalous network activity detected in Part 1.2” This language is similar to the language used in CIP-008-6.

Additionally, as described in the response to question 3, R1 uses the terminology “anomalous or unauthorized network activity” but Requirement Part 1.2 uses the term “anomalous network activity” and Part 1.3 uses the term “activity detected” with a reference back to Part 1.2. Suggest aligning this language to clarify intention and scope.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s comments. Network and metadata associated with anomalous network activity must be available for the evaluation conducted in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Network and other data associated with false positives and other detections deemed not to be malicious do not need to be further retained after the evaluation in Requirement R1, Part 1.3. However, data associated with potential attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity’s CIP-008 incident response process(es) for further investigation.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer Yes

Document Name

Comment

BHE agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Hillary Creurer - Allele - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes	0
Dislikes	0

Response

Thank you for your support. Please see responses to EEI's comments.

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment

ITC supports EEI's comments on this project.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your support. Please see responses to EEI's comments.

Daniel Gacek - Exelon - 1

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment

Exelon supports the comments submitted by the EEI for this question.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your support. Please see responses to EEI's comments.

Kinte Whitehead - Exelon - 3

Answer	Yes
Document Name	
Comment	
Exelon is aligning with the EEI in response to this question.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Since Part 1.3 requires two separate actions, SPP recommends the following edit to the proposed language in R1, Part 1.3 (i.e., "change the word "to" to "and"):	
Implement one or more method(s) to evaluate activity detected in Part 1.2 and determine appropriate action.	
Likes	0
Dislikes	0
Response	
Thank you for your support. The DT disagreed with your suggestion to change "to" to "and," but did revise Requirement R1, Part 1.3:	
1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
BHE agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).	
Likes	0
Dislikes	0
Response	
Thank you for your support.	

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC

Answer Yes

Document Name

Comment

Cleco agrees with EEI comments.

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI's comments.

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer Yes

Document Name

Comment

The way the measures for Part 1.3 are written, it appears entities could select just one. Was this the intent of the DT? Consider revising to clarify that documentation is needed for evaluating and responding to anomalous or unauthorized network activity and an escalation process linking it to CIP-008.

Likes 0

Dislikes 0

Response

Thank you for your support. Network and metadata associated with anomalous network activity must be available for the evaluation conducted in CIP-015-1, Requirement R1, Part 1.3. Network and other data associated with false positives and other detections deemed not to be malicious do not need to be further retained after evaluated in Requirement R1, Part 1.3. However, data associated with potential

attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity’s CIP-008 incident response process(es) for further investigation.

David Jendras Sr - Ameren - Ameren Services - 3

Answer Yes

Document Name

Comment

Ameren agrees with and supports EEI comments.

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI’s comments.

Richard Vendetti - NextEra Energy - 5

Answer Yes

Document Name

Comment

NEE support’s EEI’s comment(s): EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI’s comments.

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

Answer Yes

Document Name

Comment

The standard does not provide sufficient minimum expectations for what the CEA will likely find sufficient.

Likes 0

Dislikes 0

Response

Thank you for your support. Section C of the standard provides information on evidence retention.

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer Yes

Document Name

Comment

Southern Company agrees with the feedback by EEI.

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI's comments.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer Yes

Document Name

Comment

No additional comments

Likes 0

Dislikes 0

Response

Thank you for your support.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer Yes

Document Name

Comment

BPA believes there is still room for clarification to revise “anomalous network activity” to “anomalous conditions”. Network conditions can include lack of activity or states.

Likes 0

Dislikes 0

Response

Thank you for your support.

The DT considered whether or not to create a NERC Glossary term for “anomalous”. After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was unnecessary to define the term in the NERC Glossary.

Anomalous - adjective

1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification
 b: marked by incongruity or contradiction : PARADOXICAL

The DT created a FAQ document that addresses this, as well as updating the Technical Rationale document for additional clarity. Further, the DT updated Requirement R1, Parts 1.1., 1.2., and 1.3.

- 1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.
- 1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.
- 1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer Yes

Document Name

Comment

Black Hills Corporation agrees with EEI’s comments: EEI agrees that the proposed CIP-015-1 Requirement R1, Part 1.3 provides Registered Entities with flexibility to evaluate activity detected in Part 1.2 to determine appropriate action. We appreciate that the measures provide high-level guidance to achieving the risk-based approach which may, or may not, include escalation of the CIP-008 Cyber Security Incident response plan(s).

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI’s comments.

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer Yes

Document Name	
Comment	
PG&E agrees the modifications are clear on the intent.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECl	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	

Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0

Response	
Thank you for your support.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

James Keele - Entergy - 3

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

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

Answer Yes

Document Name

Comment

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Patricia Lynch - NRG - NRG Energy, Inc. - 5,6

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer Yes

Document Name

Comment

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
TFIST had no comment on question 6.	
Likes	0
Dislikes	0
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
<p>While the measures do provide guidance, the requirement language should be clear in the intent. Texas RE recommends the following language to clarify the intent of Requirement Part 1.3:</p> <p>R1.3 Implement one or more method(s) to evaluate activity detected in Part 1.2 to determine appropriate action, up to and including identifying the anomalous network activity as a Cyber Security Incident.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT updated Requirement 1, “Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity’s Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts:”</p> <p>In addition, the DT updated Requirement R1, Part 1.3, “Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).”</p>	

7. The Project 2023-03 DT has drafted Requirement R2 of proposed CIP-015-1 for Registered Entities to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification. Do you agree that the proposed CIP-015-1 Requirement R2 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Ruchi Shah - AES - AES Corporation - 5

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

AES agrees with protecting INSM data from being inadvertently deleted or modified. However, we do not want the categorization or treatment of INSM data be conflated with or mistaken for BCSI. The two types of information must be treated as two separate and discrete types of information.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. The DT agrees that the data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing⁵” should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

⁵ <https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf>

Answer	No
Document Name	
Comment	
<p>Duke Energy sees additional opportunities for clarification in R2. We are concerned that R2 is redundant for entities who will classify their INSM systems as EACMs, and that the flexibility in INSM system classification is not clear. We propose “Responsible Entity with an INSM system not classified as an EACM shall implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT agrees there may be some overlap in requirements. The intention of specifying the requirement under R2 ensures the protection is in place regardless of the categorization of the INSM system.</p>	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	No
Document Name	
Comment	
<p>Black Hills Corporation seeks clarification on \how this Requirement R2 differs from the existing CIP-011 language regarding data protection, as we would like to see a standard that does not duplicate or conflict with existing CIP requirement language.</p> <p>Black Hills Corporation also agrees with the comments from EEI: EEI proposes the following revision to CIP-015-1 R2:</p> <p>Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification (<i>remove: , except during CIP Exceptional Circumstances</i>).</p>	

As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement.

EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes	0
Dislikes	0

Response

Thank you for your support. The DT believes data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection. Additionally, please see responses to EEI’s comments.

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

R2 states to protect the traffic. The standard should be more specific on if the information should be protected in transit or at rest and the type of data that the requirements cover. The standard could confuse the data on the network with the reports or subsequent analysis coming out of the INSM data.

Furthermore, Cogentrix proposes that ISNM data be specifically added as an item for CIP-011 classification as BCSI; as a result, this requirement is not needed.

Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT agrees that the data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing⁶” should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.</p>	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	No
Document Name	
Comment	
<p>The way in which this requirement reads there are CIP-012 overtones. Protecting data against the risks of 'unauthorized deletion or modification' is too close to the goal/objective of CIP-012, creating confusion and cross-over.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT has also updated the Technical Rationale document for clarity on Requirement R2. Additionally, the DT has also created a FAQ document for this project that states, “Because network traffic captured in transit between hosts cannot typically be</p>	

⁶ <https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf>

modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.”

Robert Follini - Avista - Avista Corporation - 3

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

Avista agree with EEI comments

EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0	
---------	--

Dislikes 0	
------------	--

Response

Thank you for your comment. Please see responses to EEI’s comments.

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

Southern Company agrees with the feedback by EEI.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
<p>NEE support's EEI's comment(s): EEI proposes the following revision to CIP-015-1 R2:</p> <p>Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.</p> <p>As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement.</p> <p>EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.</p>	
Likes	0

Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #7.	
Likes	0
Dislikes	0
Response	

Thank you for your comment. Please see responses to EEI's comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy supports EEI comments.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
LCRA understands the intent of the SDT when drafting this requirement, however, LCRA is concerned that INSM data is being treated inconsistently when compared to monitoring data present on other EACMS (e.g., SIEM). Additionally, we believe that INSM data will meet the NERC Glossary of Terms definition of BCSI. Given this, it may be beneficial to add availability and integrity to Requirement 1 in CIP-011.	
Likes	0
Dislikes	0
Response	

Thank you for your comment. The DT has also created a FAQ document for this project that states, “Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.”

Additionally, the DT believes data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection. Additionally, please see responses to EEI’s comments.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

No, there are a variety of of events, logs and other evidence based output that is generated by other CIP standards that don't require this level of protection. This appears to be overreaching in the protection of data that is beyond the protection of the BCS requirements.

Likes 0	
---------	--

Dislikes 0	
------------	--

Response

Thank you for your comment. The DT has also created a FAQ document for this project that states, “Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.”

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC

Answer	No
---------------	----

Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA understands the intent of the SDT when drafting this requirement, however, LCRA is concerned that INSM data is being treated inconsistently when compared to monitoring data present on other EACMS (e.g., SIEM). Additionally, we believe that INSM data will meet the NERC Glossary of Terms definition of BCSI. Given this, it may be beneficial to add availability and integrity to Requirement 1 in CIP-011.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. The DT has also created a FAQ document for this project that states, "Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network."	

Additionally, the DT believes data may not rise to the level of BCSI and the ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” should be referenced to determine if the INSM system and its components are Protected Cyber Asset (PCA), EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection. Additionally, please see responses to EEI’s comments.

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

It is not clear if the Requirement R2 is expecting both detection of unauthorized access and/or changes along with protection mechanisms to prevent unauthorized access or if the entity can choose what combination of controls is appropriate to them based on their security risk tolerance.

BC Hydro recommends to provide clarity in the Requirement R2 to remove ambiguity and scope these accurately. BC Hydro also notes that although Technical Rationale provides examples of guidance it is not an ERO endorsed compliance guidance document. Auditors may chose to adhere to certain aspects from Technical Rationale and choose to leave others.

Likes 0	
---------	--

Dislikes 0	
------------	--

Response

Thank you for your comment. Requirement R2 has been revised to: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.”

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

EEI proposes the following revision to CIP-015-1 R2:

Responsible Entity shall implement, **except during CIP Exceptional Circumstances**, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.

As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement.

EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. Please see responses to EEI’s comments.

Robert Blackney - Edison International - Southern California Edison Company - 1

Answer	No
--------	----

Document Name	
---------------	--

Comment

See comments submitted by the Edison Electric Institute.

Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes	0
Dislikes	0
Response	

Thank you for your comment. Please see responses to EEI's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports EEI's comments on this project.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments:	
"R2 states to protect the traffic. The standard should be more specific on if the information should be protected in transit or at rest and the type of data that the requirements cover. NPCC RSC is concerned that the standard could confuse the data on the network with the reports or subsequent analysis coming out of the INSM data."	
Likes	0
Dislikes	0
Response	

Thank you for your comment. Please see responses to NPCC RSC's comments.	
Hillary Creurer - Allele - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
Does this suggest that the RE maintain the evidence? Why? For how long? What is the purpose and intent of this requirement? Could CIP-004 (access), CIP-005 (vendor access) or CIP-011 (BCSI protections) be leveraged for this purpose? Clarification is needed as it is not clear what the purpose and intent of this requirement is.	
What does "To mitigate the risk of unauthorized deletion or modification" mean? Again, shouldn't CIP-004 R4 and CIP-011 address this? Also, do the individuals who have the access, be the ones authorized to have the access. One concern is when vendors who have this access, and how would an entity monitor for such activity?	
Likes	0

Dislikes	0
Response	
<p>Thank you for your comment. Requirement R2 has been revised to: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.” The Technical Rationale has been updated to provide further clarity.</p>	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
<p>EEI proposes the following revision to CIP-015-1 R2:</p> <p>"Responsible Entity shall implement, <i>except during CIP Exceptional Circumstances</i>, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification."</p> <p>As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement.</p> <p>EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.</p>	
Likes	0
Dislikes	0
Response	

Thank you for your comment. Requirement R2 has been revised to: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.” The Technical Rationale has been updated to provide further clarity.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

BHE proposes the following clarification to CIP-015-1 R2 Technical Rationale:

BHE seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. BHE seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0

Dislikes 0

Response

Thank you for your comment. Data protection in CIP-015-1, Requirement R2, is intended to protect the data from being altered or removed by an advisory intended to cover their tracks. BCSI protection as defined in the CMEP guide and CIP-011 is to protect against data or information that could be used to gain unauthorized access to a BES Cyber System.

Bret Galbraith - Seminole Electric Cooperative, Inc. - 6

Answer No

Document Name

Comment

Seminole agrees the EEI

EEI Response:

Responsible Entity shall implement, **except during CIP Exceptional Circumstances**, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.

As written, the language could suggest that an entity does not need to protect the INSM data from unauthorized deletion or have a process for protecting it if they declare a CIP Exceptional Circumstance. Moving the CEC language up in the requirement more clearly aligns with the intention of the requirement.

EEI seeks additional clarity in the Technical Rationale related to the protections for INSM data and BCSI. Page 3 of the Technical Rationale refers to the CMEP Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” and notes that the Entities may be required to apply BCSI protections to INSM systems and its components. EEI seeks clarification of the similarities and differences between BCSI protections and those required under CIP-015-1 Requirement R2.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s comments.

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer Yes

Document Name

Comment

PG&E agrees the modifications are clear on the intent.

Likes 0

Dislikes 0

Response

Thank you for your support.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer Yes

Document Name

Comment

BPA believes there is an operational concern that logs should be set to over-write rather than causing a full disk stop condition. This may be a higher priority than keeping all logs, as the proliferation of security event logs, in itself, is an indicator of an issue that can feed into response activities.

Likes 0

Dislikes 0

Response

Thank you for your support. The DT has revised Measure M2: Evidence may include, but is not limited to, documentation demonstrating how data is being protected from the risk of unauthorized deletion or modification.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer Yes

Document Name

Comment

No additional comments

Likes 0

Dislikes 0

Response

Thank you for your support.

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

Answer Yes

Document Name

Comment

The protection of the data does not need additional standards since a risk has not been identified that this newly created data element is subject to. Why would this data be subject to risk of unauthorized deletion or modification compared to other security logs or data?

Likes 0

Dislikes 0

Response

Thank you for your support. Project 2023-03 INSM is addressing FERC Order No. 887.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer Yes

Document Name

Comment

The NAGF recommends placing the following statement “except during CIP Exceptional Circumstances” after the word implement which specifies the action for the phrase rather than a general statement.

Likes	0
Dislikes	0
Response	
Thank you for your support. The updated requirement reads: Requirement R2: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.”	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
BHE proposes the following clarification to CIP-015-1 R2 Technical Rationale:	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes	0

Dislikes	0
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer

Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Andrew Smith - APS - Arizona Public Service Co. - 5

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer Yes

Document Name

Comment

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Amy Wilke - American Transmission Company, LLC - 1

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Alain Mukama - Hydro One Networks, Inc. - 1

Answer Yes

Document Name

Comment

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECl	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
R2 states to protect the traffic. The standard should be more specific on if the information should be protected in transit or at rest and the type of data that the requirements cover. TFIST is concerned that the standard could confuse the data on the network with the reports or subsequent analysis coming out of the INSM data	
Likes	0
Dislikes	0
Response	

Thank you for your support. The DT has revised Requirement R2 to: “Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.” The DT has also updated the Technical Rationale document for clarity on Requirement R2.

Additionally, the DT has also created a FAQ document for this project that states, “Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.”

8. The Project 2023-03 DT has drafted Requirement R3 of proposed CIP-015-1 for Registered Entities to retain network communications data and other meta data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, which is the evaluation of anomalous activity in order to determine appropriate action. The goal of the Project 2023-03 DT was to allow Registered Entities to determine how to meet the objectives without defining strict duration that could cause the retention of substantial amounts of data that may not be relevant to meeting the security objects of the Reliability Standard. Do you agree that the proposed CIP-015-1 Requirement R3 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Bret Galbraith - Seminole Electric Cooperative, Inc. – 6

Answer

No

Document Name

Comment

Seminole Agrees with the comments from MRO NSRF

MRO NSRF is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. MRO NSRF believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, MRO NSRF suggests modifying Requirement parts R1.2 and R1.3 to read:

1.2. Implement one or more method(s) to detect and alert on anomalous network activity using the data collected at locations identified in Part 1.1

1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to determine if a Cyber Security Incident has occurred.

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this MRO NSRF suggests eliminating CIP-015 R3 and adding a new sub part 1.4 a to read:

1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall initiate activities identified in its Cyber Security Incident response plan.

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. Please see responses to MRO NSRF’s comments.

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	No
---------------	----

Document Name	2023-03_Comment_Form_MRO_NS RF_20240313_Final.docx
----------------------	--

Comment

MRO NSRF is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. MRO NSRF believes that the data to be retained should be limited to network

communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, MRO NSRF suggests modifying Requirement parts R1.2 and R1.3 to read:

1.2. Implement one or more method(s) to detect and alert on anomalous network activity using the data collected at locations identified in Part 1.1.

1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to determine if a Cyber Security Incident has occurred.

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this MRO NSRF suggests **eliminating CIP-015 R3** and **adding a new sub part 1.4** a to read:

1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall initiate activities identified in its Cyber Security Incident response plan.

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT made the following changes that we believe will hopefully address the concerns listed.</p> <ul style="list-style-type: none"> The DT added a note to R3 stating: <p>“Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.”</p> The DT is hesitant to have potential overlap with an entity’s existing CIP-008 processes. We altered Part 1.3 to state: <p>“Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine further action(s).”</p> <p>The implication is that anomalous activity will require a response that could range from tuning software if the activity is noise to escalating into the CIP-008 process if it could potentially be a Cyber Security Incident or attempt to compromise.</p> 	
Jennifer Neville - Western Area Power Administration – 6	
Answer	No
Document Name	
Comment	
<p>Concerns with the language in R3. The amount of data to be collected and stored is extremely voluminous, which in turn is a very expensive administrative burden that does not provide additional security or reliability. Suggest modifying the language for R1.2 and R1.3 to reflect limiting the data retained to network communications and other related data as part of the investigated alert.</p>	
Likes	0
Dislikes	0

Response

Thank you for your comment. The DT made the following change that we believe will hopefully address the concern listed.

- A note has been added to R3 stating:

“Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.”

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp – 6

Answer No

Document Name

Comment

BHE is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored for extended periods of time. BHE proposes revising the draft R3 language as follows:

“Responsible Entity shall implement one or more documented process(es) to retain, **with sufficient detail for at least ninety days**, INSM data **evaluated** in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances.”

The choice for “ninety days” duration is meant to keep consistency with other CIP Standard log retention requirements.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT made the following change that we believe will hopefully address the concern listed.

A note has been added to R3 stating:

“Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.”

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer No

Document Name

Comment

EEl is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEl proposes revising the draft R3 language as follows:

“Responsible Entity shall implement one or more documented process(es) to retain, **with sufficient detail and duration, INSM data evaluated in support of** Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances.”

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT made the following change that we believe will hopefully address the concern listed.

- Requirement R3 was revised to the following:

“Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.”

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
<p>The phrase "retain network communications data AND other metadata." This insinuates that entities may need full PCAP monitoring of an entire BCS and retaining entire conversations. This could require significant allocation of resources from entities, especially if storage is required for a significant amount of time. Entities should be able to establish retention requirements in their program for full PCAP if required to implement as this approach may not be cost effective for entities.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT made the following change that we believe will hopefully address the concern listed.</p> <p>Requirement R3 was revised to the following:</p> <p>“Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment] Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.”</p>	
<p>Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez</p>	
Answer	No
Document Name	
Comment	

It is unclear as to how to meet any objectives of this requirement. Again, the word anomalous needs clarification. The way the requirement is written is still vague in determining how long to retain network communications data and meta data collected with sufficient detail and duration to support the analysis. The technical guidelines has more in-depth information on what should and can be the length of time. However, as we all know, auditors will be auditing to the Standard and requirements and not the technical rational. Maybe include additional information in the measures section?

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT made the following change that we believe will hopefully address the concern listed.

Requirement R3 was revised to the following:

“Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]
 Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.”

The DT considered whether or not to create a NERC Glossary term for “anomalous.” After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective

1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification

b: marked by incongruity or contradiction : PARADOXICAL

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
Document Name	
Comment	
<p>ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed.</p> <p>Requirement R3 has been revised to the following:</p> <p>Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]</p> <p>Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.</p>	
<p>Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter</p>	
Answer	No
Document Name	
Comment	
<p>The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive. The data to be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other</p>	

related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

Consider:

R3: Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data with sufficient detail and duration collected as part of the response to an investigated alert initiated from the analysis performed in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Katrina Lyons - Georgia System Operations Corporation - 4

Answer No

Document Name

Comment

Georgia System Operations Corporation supports ACES comments: "ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc."

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to ACES' comments.

Hillary Creurer - Allele - Minnesota Power, Inc. - 1

Answer No

Document Name

Comment

Minnesota Power supports EEI's comments.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer No

Document Name

Comment

OPG supports NPCC Regional Standards Committee's comments:

"R3 The standard is not clear on a timeline for assessment or how long the INSM information should be retained or a timeline for assessment. NPCC RSC is unclear on what "sufficient detail and duration" means and if these words are necessary."

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to NPCC RSC's comments.

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer No

Document Name

Comment

ITC supports EEI's comments on this project.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.

Daniel Gacek - Exelon - 1

Answer No

Document Name

Comment

Exelon supports the comments submitted by the EEI for this question.

Likes 0

Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is aliging with the EEI in response to this question.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP asks that the SDT provide additional clarity around (i) what is a reasonable duration for network communications data and metadata retention, and what is defined as network communications data and metadat	
Likes	0
Dislikes	0
Response	

Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	
Comment	
It is unclear on how long the data needs to be retained. Suggest including a clear timeline minimum 90 days to match with CIP-007 R4.3 event Log retention	
Likes	0
Dislikes	0

Response

Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Robert Blackney - Edison International - Southern California Edison Company - 1

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

See comments submitted by the Edison Electric Institute.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. Please see responses to EEI's comments.

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows:

“Responsible Entity shall implement one or more documented process(es) to retain, **with sufficient detail and duration**, network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances.”

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s comments.

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer No

Document Name

Comment

BC Hydro has concerns about the extensive data volume and high costs associated with Requirement R3 per the current language. BC Hydro suggests limiting retained data to network communications and relevant information linked to investigated alerts only. A full capture of network data poses excessive burdens in terms of cost and sustainment and does not contribute extensively in enhancing security or reliability for the Bulk Electric System. BC Hydro recommends that the DT narrow the scope of INSM (Internal Network Security Monitoring) data to only Attempt to Compromises and reportable Cyber Security Incidents only in line with CIP-008 requirements.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer No

Document Name

Comment

BHE is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored for extended periods of time. BHE proposes revising the draft R3 language as follows:

“Responsible Entity shall implement one or more documented process(es) to retain, **with sufficient detail for at least ninety days**, network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances.”

The choice for “ninety days” duration is meant to keep consistency with other CIP Standard log retention requirements.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC

Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes	0
Dislikes	0

Response

Thank you for your comment. Please see responses to EEI's comments.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer	No
Document Name	
Comment	

No, NCPA agrees with AES statement.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to AES's comments.

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

Answer No

Document Name

Comment

Dominion Energy supports EEI comments.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer No

Document Name

Comment

AEPC has signed on to ACES comments:

ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to ACES' comments.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer No

Document Name

Comment

NST believes R3 should clarify it is left to Registered Entities to decide what collected data should be retained and for how long. We suggest, "Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data collected with sufficient detail and duration, *as determined by the Responsible Entity*, to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances."

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.	
Likes	0
Dislikes	0

Response

Thank you for your comment. Please see responses to IRC SRC's comments.

David Jendras Sr - Ameren - Ameren Services - 3

Answer	No
Document Name	
Comment	
Ameren agrees with and supports EEI comments.	
Likes	0
Dislikes	0

Response

Thank you for your comment. Please see responses to EEI's comments.

Roger Perkins - Southern Maryland Electric Cooperative - 1

Answer No

Document Name

Comment

SMECO agrees with ACES comments:

ACES agrees with the way R3 is written, but the requirement is not specific to how long an entity would be required to retain network communications data and other meta data collected for an actual incident. ACES believes the requirement should be explicit for data retention for an actual incident such as audit period, 36 months, etc.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to ACES' comments.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer No

Document Name

Comment

The SRC recommends that the standard be revised to provide additional clarity regarding the extent of a Responsible Entity's ability to define and determine what data (particularly metadata) needs to be retained and the appropriate retention period. Without additional clarity, the

SRC is concerned that Requirement R3 could be construed to require entities to retain large amounts of data for the full duration of the three-year evidence retention period applicable to CIP-015-1.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Richard Vendetti - NextEra Energy - 5

Answer No

Document Name

Comment

NEE support's EEI's comment(s): EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows:

“Responsible Entity shall implement one or more documented process(es) to retain, **with sufficient detail and duration**, network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances.”

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s comments.

Andrew Smith - APS - Arizona Public Service Co. - 5

Answer No

Document Name

Comment

AZPS agrees with EEI’s concerns regarding the proposed language for CIP-015-1 R3. Potential ambiguity in the current draft of data collection requirements may lead to interpretations which require significant data collection and storage. AZPS supports the following revised language:

“Responsible Entity shall implement one or more documented process(es) to retain, **with sufficient detail and duration**, network communications data and other meta data INSM data collected with sufficient detail and duration **evaluated** to support the analysis in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances.”

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s comments.

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	
Comment	
Southern Company agrees with the feedback by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Avista agrees with EEI's comment -- EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see responses to EEI's comments.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	

Comment

*“R3 Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data collected **with sufficient detail and duration** to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.”*

The bolded part (“with sufficient detail and duration”) is unquantifiable and can potentially be too subjective. LDWP would recommend specific criteria or additional technical guidance be included for what “sufficient detail and duration” entails.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer	No
--------	----

Document Name	
---------------	--

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to MRO NSRF’s comments.

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF

Answer No

Document Name

Comment

R3 The standard is not clear on a timeline for assessment or how long the INSM information should be retained or a timeline for assessment. This brings the question of what “sufficient detail and duration” means and are these words necessary? Further, other approved CIP standards offer specific data retention periods. Cogentrix does not believe this ambiguity is helpful to the objective and the DT should specify a timeframe to help clarify entity expectations and introduce consistency in application.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer No

Document Name

Comment

Black Hills Corporation agrees with EEI’s comments: EEI is concerned that the proposed CIP-015-1 Requirement R3 does not clearly limit the scope of data required to be collected and stored by the Responsible Entity, which could lead to voluminous amounts of data being collected and stored leading to unintended cost implications. EEI proposes revising the draft R3 language as follows:

“Responsible Entity shall implement one or more documented process(es) to retain, **with sufficient detail and duration**, (*remove*: network communications data and other meta data) INSM data (*remove*: collected with sufficient detail and duration) **evaluated** (*remove*: to support the analysis) in support of Requirement 1, Part 1.3 **and determined by the Responsible Entity to be anomalous and require action**, except during CIP Exceptional Circumstances.”

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see response to EEI’s comments.

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer No

Document Name

Comment

The proposed language in R1 1.3 and R3 is ambiguous and should be revised. Implementation time frame is too restrictive taking into consideration the substantial efforts and undertaking of this project.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Donna Wood - Tri-State G and T Association, Inc. - 1

Answer

No

Document Name

Comment

Tri-State agrees with the comments below:

AES is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive.

AES believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, [Member] suggests modifying Requirement parts R1.2 and R1.3 to read:

1.2. Implement one or more method(s) to detect **and alert** on anomalous network activity using the data collected at locations identified in Part 1.1.

1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to **determine if a Cyber Security Incident has occurred.**

Based on the determination made in 1.3, AES suggests two options:

Option 1:

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its CIP-008 Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this [Member] suggests eliminating CIP-015 R3 and adding a new sub part 1.4 a to read:

1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall initiate activities identified in its CIP-008 Cyber Security Incident Response Plan.

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. Please see response to AES.

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF

Answer	No
Document Name	
Comment	
<p>Duke Energy suggests additional clarification on the retention expectation for R3 and removal of the language “sufficient detail and duration”. We would suggest this alternative language “Responsible Entity shall implement one or more documented process(es) to retain network communications data collected to complete the analysis in Requirement R1, Part 1.3 and to execute their Cyber Security Incident response plan where required.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT has made the following change that we believe will hopefully address the concern listed.</p> <p>Requirement R3 has been revised to the following:</p> <p>Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]</p> <p>Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.</p>	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	No
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Is there an intended difference between “INSM data collected” as referenced in R2 when compared to “network communications data and other meta data collected” as referenced in R3? If this is the same thing, ATC supports the intent of the requirement, but requests consideration of using consistent terminology for clarity.	
Likes	0
Dislikes	0
Response	
Thank you for your support. The current revision of R2 addresses the concerns that you listed above:	
R2. Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3 to mitigate the risks of unauthorized deletion or modification.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	

LCRA would like to acknowledge that storage capability will most likely be a function of cost. Additionally, establishing bright-line parameters for length of time data should be kept could present challenges to entities due to the dynamic nature of logging and alerting. Scenarios may exist when storage becomes full after only 3 months when it typically takes 12.

This will likely be more of a function of cost versus want. Depending on number of alerts and need to keep for entire audit period.

Likes 0

Dislikes 0

Response

Thank you for your support. The DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer Yes

Document Name

Comment

LCRA would like to acknowledge that storage capability will most likely be a function of cost. Additionally, establishing bright-line parameters for length of time data should be kept could present challenges to entities due to the dynamic nature of logging and alerting. Scenarios may exist when storage becomes full after only 3 months when it typically takes 12.

Likes	0
Dislikes	0
Response	
<p>Thank you for your support. The DT has made the following change that we believe will hopefully address the concern listed.</p> <p>Requirement R3 has been revised to the following:</p> <p>Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]</p> <p>Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.</p>	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
<p>PNMR agrees with R3, but to more closely align with R2, which states entities must protect INSM Data, PNMR believes the language of R3 should read:</p> <p>“Responsible Entity shall implement one or more documented process(es) to retain internal network security monitoring data collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.”</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your support and comments. The DT has made the following change that we believe will hopefully address the comment listed.</p>	

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

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

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment	
----------------	--

The standard does not provide sufficient minimum expectations for what the CEA will likely find sufficient.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your support and comments. The DT has made the following change that we believe will hopefully address the comment listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer Yes

Document Name

Comment

No additional comments

Likes 0

Dislikes 0

Response

Thank you for your support.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer Yes

Document Name

Comment

BPA recommends that a suggested minimum retention parameter be included in the Technical Rationale. BPA believes this would be in alignment with language cited in CIP-007 R4, 90-day event log retentions.

Likes 0

Dislikes 0

Response

Thank you for your support and comments. The DT has made the following change that we believe will hopefully address the comment listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment	
----------------	--

PG&E agrees the modifications are clear on the intent.

Likes 0	
---------	--

Dislikes 0	
------------	--

Response	
-----------------	--

Thank you for your support.

Colin Chilcoat - Invenergy LLC - 6

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment	
----------------	--

Likes 0	
---------	--

Dislikes	0
Response	
Thank you for your support.	
Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0

Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

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

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
R3 The standard is not clear on a timeline for assessment or how long the INSM information should be retained or a timeline for assessment.	
TFIST is unclear on what “sufficient detail and duration” mean and if these words are necessary.	
Likes	0

Dislikes 0

Response

Thank you for your comment. The DT has made the following change that we believe will hopefully address the comment listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE is concerned that not establishing guidelines or thresholds for minimum retention periods, this requirement would be a challenge to comply with, audit, and enforce consistently. Texas RE notes that FERC Order No. 887 specifically identifies the need to “maintain . . . logs, and other data collected, regarding network traffic” as key security objective for the implementation of an effective INSM program. Failure to maintain evidence of the collection of log data renders this security objective essentially unenforceable.

Texas RE concedes that a blanket requirement to retain logs may not be appropriate to meet this security objective. For example, from a storage perspective it would be very expensive to require network traffic of full system backups to be stored for 90 days. Likewise, from a threat perspective this is known and expected traffic and would be of minimal benefit to store. As such, Texas RE recommends adding language to the requirement for Registered Entities to explicitly define types of traffic that will not be required to be retained. Registered Entities could write into their program that expected traffic will be excluded from storage and retention requirements. However, this

expectation should be clear from the requirement language itself, and the burden placed on entities to carefully define and demonstrate they are accomplishing the FERC-mandated security objective to retain maintain sufficient logs regarding network traffic so that can detect anomalous events and effectively demonstrate compliance with that expectation.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Ruchi Shah - AES - AES Corporation - 5

Answer

Document Name

Comment

AES is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle would be extremely voluminous and overly expensive.

AES believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, [Member] suggests modifying Requirement parts R1.2 and R1.3 to read:

*1.2. Implement one or more method(s) to detect **and alert** on anomalous network activity using the data collected at locations identified in Part 1.1.*

*1.3. Implement one or more method(s) and evaluate activity detected in Part 1.2 to **determine if a Cyber Security Incident has occurred**.*

Based on the determination made in 1.3, AES suggests two options:

Option 1:

Where the evaluation of detected anomalous or unauthorized network activity made in Part 1.3 is determined to be a Cyber Security Incident, the Responsible Entity shall initiate activities identified in its CIP-008 Cyber Security Response Plan. By doing this we would eliminate the potential for double jeopardy with duplicative Requirements in CIP-008 and CIP-015. To achieve this [Member] suggests eliminating CIP-015 R3 and adding a new sub part 1.4 a to read:

1.4. When detected anomalous or unauthorized network activity is determined to be a Cyber Security Incident (reportable or attempt to compromise), the Responsible Entity shall initiate activities identified in its CIP-008 Cyber Security Incident Response Plan.

The existing CIP-008 activities would include a response or mitigation of the Cyber Security Incident (CIP-008 R1.1) identified as a result of the activities performed in CIP-015-1 R1. CIP-008 R2.3 would also include activities needing to be performed to address data collection and retention of network communications data and other meta data that is currently proposed in CIP-015-1 R3.

Option 2:

If the DT does not agree with Option 1, AES suggests modifying R3 to read:

*R3: Responsible Entity shall implement one or more documented process(es) to retain network communications data and other meta data with sufficient detail and duration **collected as part of the response to an investigated alert initiated from the analysis performed in Requirement R1, Part 1.3**, except during CIP Exceptional Circumstances.*

Likes	0
Dislikes	0

Response

Thank you for your comment. The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following changes that we believe will hopefully address the concerns listed.

- Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

- Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.
- The DT is hesitant to have potential overlap with an entity's existing CIP-008 processes. We have altered Part 1.3 to state:

“Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2 to determine further action(s).”

The implication is that anomalous activity will require a response that could range from tuning software if the activity is noise to escalating to the CIP-008 process if it could potentially be a Cyber Security Incident or attempt to compromise.

9. Do you agree with the Implementation Plan for proposed CIP-015-1 that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Ruchi Shah - AES - AES Corporation - 5

Answer No

Document Name

Comment

AES agrees with the proposed Implementation Plan but would not support a shorter timeline for Control Centers or applicable BCS.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer No

Document Name

Comment

No, Southern Indiana Gas & Electric (SIGE) does not agree with the implementation plan because implementation in generation and substation facilities will be extremely time consuming. Implementation within a high or medium Control Center will also be time consuming in

order to ensure communications are not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. SIGE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer No

Document Name

Comment

No, CenterPoint Energy Houston Electric (CEHE) does not agree with the implementation plan because implementation in substation facilities will be extremely time consuming. Implementation within a high impact Control Center will also be time consuming in order to ensure communications are not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. CEHE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

Implementation time frame is too restrictive taking into consideration the substantial efforts and undertaking of this project.. The undertaking will demand significant effort, substantial capital investment and additional staffing.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

BPA reiterates its comments from the previous comment period regarding the proposed implementation plan timeline.

BPA's previous comments: "After reviewing the new requirement language in CIP-015-1, BPA believes more time will be required to implement an INSM program. This takes into consideration the initial effort needed to create new processes and plans for INSM, procure new equipment (availability of vendors, products, and potential supply chain issues), modify networks, gather network information, and implement capabilities to consume network information and perform the necessary analysis. With that said, BPA recommends the SDT revise the implementation plan to state '60 months for high impact cyber systems (located at Control Centers and backup Control Centers), with an additional 24 months for medium impact cyber systems with ERC.'"

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer No

Document Name

Comment

Southern Company agrees with the feedback by EEI.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
This Standard's implementation as drafted can be very time and cost intensive due to language in R3 as commented in response to Question #8 above.	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.</p> <p>Lastly, the DT would remind entities that FERC issued Order Nos. 893 and 893-A in 2023, which provide <i>Incentives for Advanced Cyber security Investment</i> as directed by the Infrastructure Investment and Jobs Act of 2021. The Order establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the Order as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.</p>	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No

Document Name	
Comment	
SRP would need for the questions above to be answered and the standard to be clearer before we can make a determination on a timeline. Currently the standard is written as a Subjective standard vs. an Objective standard and additional clarity would be needed.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the Implementation Plan timing.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	

Black Hills Corporation agrees with EEI comments: EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

Likes 0

Dislikes 0

Response

Thank you for your support.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer Yes

Document Name

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum.

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to MRO NSRF's comments.

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer Yes

Document Name

Comment

MRO NSRF agrees with the proposed Implementation Plan but would not support a shorter timeline for Control Centers or applicable BCS.

Likes 0

Dislikes 0

Response

Thank you for your support. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter

Answer Yes

Document Name

Comment

No additional comments

Likes 0

Dislikes 0

Response

Thank you for your support.

Richard Vendetti - NextEra Energy - 5

Answer Yes

Document Name

Comment

NEE support's EEI's comment(s): EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI's comments.

David Jendras Sr - Ameren - Ameren Services - 3

Answer Yes

Document Name

Comment

Ameren agrees with and supports EEI comments.

Likes 0

Dislikes 0

Response

Thank you for your support. Please see responses to EEI's comments.

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer Yes

Document Name

Comment

BHE agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

Likes 0

Dislikes 0

Response

Thank you for your support. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

Glen Farmer - Avista - Avista Corporation - 5

Answer Yes

Document Name

Comment

EI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

Likes 0

Dislikes	0
Response	
<p>Thank you for your support. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.</p>	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
<p>See comments submitted by the Edison Electric Institute.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your support. Please see responses to EEI's comments.</p>	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
<p>Exelon is aliging with the EEI in response to this question.</p>	
Likes	0

Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this question.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports EEI's comments on this project.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
<p>OPG supports NPCC Regional Standards Committee's comments: "NPCC RSC agrees with the implementation plan."</p>	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to NPCC SRC's comments.	
Hillary Creurer - Allele - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to EEI's comments.	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes

Document Name	
Comment	
Georgia System Operations Corporation supports ACES comments: "While ACES does not oppose a 36 month implementation plan, ACES believes the INSM OT industry and ERO lack sufficient SMEs to get this implemented fully by all entities across the ERO in 36 months. ACES feels there needs to be an extension provision in the implementation plan."	
Likes	0
Dislikes	0
Response	
Thank you for your support. Please see responses to ACES' comments.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	Yes
Document Name	
Comment	
Constellation feels strongly that more than 18 calendar months is needed for implementation.	
Likes	0
Dislikes	0
Response	
Thank you for your support. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
<p>EEI agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your support. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.</p>	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
<p>BHE agrees with the proposed CIP-015-1 Implementation Plan that requires compliance within 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers as it supports Registered Entities ability to prioritize implementation in accordance with reliability risk, and considers the challenges posed by the limited pool of</p>	

vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.

Likes 0

Dislikes 0

Response

Thank you for your support.

Martin Sidor - NRG - NRG Energy, Inc. - 5,6

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Gail Golden - Entergy - Entergy Services, Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
C. A. Campbell - LS Power Development, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jason Chandler - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Andrew Smith - APS - Arizona Public Service Co. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Thank you for your support.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your support.

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

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your support.

Jennie Wike - Jennie Wike On Behalf of: Hien Ho, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; John Nierenberg, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Ozan Ferrin, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; Terry Gifford, Tacoma Public Utilities (Tacoma, WA), 1, 4, 5, 6, 3; - Jennie Wike, Group Name Tacoma Power

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer Yes

Document Name

Comment

Likes 0

Dislikes 0

Response

Thank you for your support.

Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi

Answer Yes

Document Name

Comment

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes	0
Dislikes	0
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECl	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
WECC defers to the comments by the applicable entites on the Implementation Plan	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	

Was not discussed on 3/7/2024 meeting.

Likes 0

Dislikes 0

Response

Thank you for your comment.

10. Do you agree that the proposed CIP-015-1 is a cost-effective way to meet the reliability goal/FERC directives? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer No

Document Name

Comment

Current proposed version and changes leave technical requirements not defined enough to allow BHE to determine whether there is a way to meet CIP-015 with a cost-effective implementation.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECl

Answer No

Document Name

Comment

More clarity within the requirements is needed to determine cost-effectiveness of needed controls.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT has made revisions to proposed Reliability Standard CIP-015-1 based on industry comments.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

This standard will require substantial investments in infrastructure to accomplish the monitoring objects, as well as additional personnel to provide adequate monitoring coverage and support of these systems and associated compliance requirements. A more flexible standard that incorporates monitoring from the endpoint would align more closely with existing security monitoring initiatives. Cost-effectiveness is not possible to determine with the limited clarifications at this time. More information is needed.

Likes 0	
---------	--

Dislikes 0	
------------	--

Response

Thank you for your comment. The DT would remind entities that FERC issued Order Nos. 893 and 893-A in 2023, which provide *Incentives for Advanced Cyber security Investment* as directed by the Infrastructure Investment and Jobs Act of 2021. The Order establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the Order as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds,

cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect

Likes 0

Dislikes 0

Response

Thank you for your comments. Project 2023-03 INSM was created in response to FERC Order No. 887.

Katrina Lyons - Georgia System Operations Corporation - 4

Answer No

Document Name

Comment

Georgia System Operations Corporation supports ACES comments:

"ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds, cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect the intrusion using INSM. A Mandiant IT administrator questioned an odd request for MFA credentials and through the investigation of the request, Mandiant discovered a much larger issue.

INSM is also riddled with false positives and will require more SMEs, especially at smaller Entities which are already resource constrained.

To really answer if this is cost effective the ERO would need to know:

The risk needing to be reduced or closed

How long it will take the ERO OT system vendors to get in line with the ERO from an INSM baseline communications perspective

How much vendors will increase prices due to INSM requirements
 Implementation capital cost
 Annual Operation and Maintenance cost
 How many vendors whom can perform the implementations before causing the INSM market costs to soar due to the 36 month implementation plan
 Market analysis of SMEs needed to manage INSM as required"

Likes 0

Dislikes 0

Response

Thank you for your comments. Project 2023-03 INSM was created in response to FERC Order No. 887.

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer No

Document Name

Comment

SPP asks the SDT to consider the potential cost that may arise from the scope of these requirements. As noted in other supporting documents related to INSM, the costs associated with capturing, analyzing, managing, and storing of all INSM data and metadata for any length of time will be substantial

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability

Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

Lastly, the DT would remind entities that FERC issued Order Nos. 893 and 893-A in 2023, which provide *Incentives for Advanced Cyber security Investment* as directed by the Infrastructure Investment and Jobs Act of 2021. The Order establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the Order as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

Please refer to comments in Question #8 above.

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your comment. Please see responses to Question 8.

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	No
---------------	----

Document Name	
----------------------	--

Comment

Current proposed version and changes leave technical requirements not defined enough to allow BHE to determine whether there is a way to meet CIP-015 with a cost-effective implementation.

Likes	0
Dislikes	0
Response	
Thank you for your comment.	
Chris Carnesi - Chris Carnesi On Behalf of: Dennis Sismaet, Northern California Power Agency, 4, 6, 3, 5; - Chris Carnesi	
Answer	No
Document Name	
Comment	
No, NCPA would need further analysis to detertime the cost effecivness of the proposed standard.	
Likes	0
Dislikes	0
Response	
Thank you for your comment.	
Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
<p>AEPC has signed on to ACES comments:</p> <p>ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds, cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the</p>	

most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect the intrusion using INSM. A Mandiant IT administrator questioned an odd request for MFA credentials and through the investigation of the request, Mandiant discovered a much larger issue.

INSM is also riddled with false positives and will require more SMEs, especially at smaller Entities which are already resource constrained.

To really answer if this is cost effective the ERO would need to know:

1. The risk needing to be reduced or closed
2. How long it will take the ERO OT system vendors to get in line with the ERO from an INSM baseline communications perspective
3. How much vendors will increase prices due to INSM requirements
4. Implementation capital cost
5. Annual Operation and Maintenance cost
6. How many vendors whom can perform the implementations before causing the INSM market costs to soar due to the 36 month implementation plan
7. Market analysis of SMEs needed to manage INSM as required

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to ACES' comments.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer

No

Document Name

Comment

GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer

No

Document Name

Comment

ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to IRC SRC's comments.

Roger Perkins - Southern Maryland Electric Cooperative - 1

Answer

No

Document Name

Comment

SMECO agrees with ACES comments:

ACES is still looking for the gap this standard is going to close or reduce. No quantitative or qualitative analysis have been provided to industry. There is a report that states there is a potential threat which has always been there. We do not feel leaning on the Solarwinds,

cited in the SAR, supply chain incident as a measure to introduce INSM to the CIP standards is the right direction. Solarwinds has INSM and they didn't detect the intrusion. Microsoft was also hit in the incident, has INSM, but also did not detect the intrusion. Mandiant, one of the most respected cybersecurity firms in the world, was also hit by the incident. Mandiant had their crown jewels stolen and they have INSM. Mandiant, also the discoverer of the intrusion, did not detect

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to ACES' comments.

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer No

Document Name

Comment

The SRC is concerned that the issues identified in its responses to questions 4 and 8 could materially impact the cost of meeting the underlying reliability goal and FERC directives. Specifically, if Requirement R1 is not clarified as discussed in the SRC's response to question 4, Responsible Entities may have to incur costs to upgrade or replace equipment that uses nonstandard communication protocols for which no effective INSM technology exists. If Requirement R3 is not clarified as discussed in the SRC's response to question 8, Responsible Entities may need to incur the costs of storing large quantities of data for the duration of the three-year CIP-015-1 evidence retention period.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT made revisions in the requirements based on industry's comments.

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

Answer No

Document Name	
Comment	
<p>Reclamation recommends minimizing churn among standard versions and clearly identify the scope; Reclamation also recommends the DT take additional time to coordinate the modifications with other existing drafting teams for related standards. This will help minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. Reclamation will need more information to adequately assess the cost effectiveness of the proposed approach.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comments. Project 2023-03 INSM was created in response to FERC Order No. 887.</p>	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	
Comment	
<p>Without further study the costs associated cannot be determined at this time.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment.</p>	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No

Document Name	
Comment	
PG&E does not have any current way to judge the cost-effectiveness of these requirements until the modifications have been approved.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
No, without further study, CEHE believes the costs associated with the new requirements cannot be determined. Some substation facilities will require equipment replacement in order to meet these requirements. It may take an unknown number of man-hours to evaluate and identify collection locations and methods to collect data. Entities will most likely have to add additional personnel in order to maintain compliance with the ongoing requirements to review the data collected for anomalous activity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	

Comment

No, without further study, SIGE believes the costs associated with the new requirements cannot be determined. Some generation and substation facilities will require equipment replacement in order to meet these requirements. It may take an unknown number of man-hours to evaluate and identify collection locations and methods to collect data. Entities will most likely have to add additional personnel in order to maintain compliance with the ongoing requirements to review the data collected for anomalous activity.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6

Answer No

Document Name

Comment

NIPSCO has not determined whether this will be cost effective. The procurement process for a tool(s) and resources will be initiated should the requirement language remain as is.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Ruchi Shah - AES - AES Corporation - 5

Answer No

Document Name

Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Dependent on product purchased, staff augmentation, and size of utility, the impact of the cost to implement INSM would vary greatly.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support and comment.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comments	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Colin Chilcoat - Invenergy LLC - 6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Teresa Krabe - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Thank you for your support.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your support.

Andrew Smith - APS - Arizona Public Service Co. - 5

Answer	Yes
---------------	-----

Document Name	
----------------------	--

Comment

Likes	0
-------	---

Dislikes	0
----------	---

Response

Thank you for your support.

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

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes	0
Response	
Thank you for your support.	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Alyssia Rhoads - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Thank you for your support.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	

Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes	0
Dislikes	0
Response	
Thank you for your support.	
Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter	
Answer	
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes	0
Dislikes	0

Response

Thank you for your support.

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5

Answer

Document Name

Comment

Was not discussed on 3/7/2024 meeting.

Likes 0

Dislikes 0

Response

Thank you for your support.

Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP

Answer

Document Name

Comment

WECC defers to the comments by the applicable entites on the Cost Effectiveness of the Standard.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer	
Document Name	
Comment	
NST lacks the information necessary to comment on this question.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
Ameren has no comment on the cost effectiveness of the project.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	

NEE does not comment on cost.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer

Document Name

Comment

BPA reiterates its comments from the previous comment period regarding cost-effectiveness.

BPA's previous comments: BPA cannot determine cost effectiveness at this point. It is difficult to make such a determination when new/revised requirements may constitute the acquisition of new technology, equipment, and staff training.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer

Document Name

Comment

MRO NSRF has no comment on the cost effectiveness of the proposed changes.

Likes 0

Dislikes 0

Response

Thank you for your comment.

C. A. Campbell - LS Power Development, LLC - 5

Answer

Document Name

Comment

No. From a generation facility perspective, this would be a heavy lift and substantial cost burden. As indicated on the INSM survey submitted last year, owners with multiple assets (especially generaiton) do not have baked-in cost recovery mechanisms. LS Power Development recommends referring to survey responses, specifically those from GO/GOPs. IT/OT support services at the plant level is a relatively newer initiative, and network infrastructure requirements per CIP-015 (though practical and good cyber security practice) are still crippling cost-wise. Other than performing a study to realize the actual risks to generation facilities, there presently isn't sufficient justificaition.

Likes 0

Dislikes 0

Response

Thank you for your comment. Project 2023-03 INSM was created in response to FERC Order No. 887. The DT provided an implementation timeframe of 36 months for high impact and medium impact with ERC control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those locations which may be more challenging to implement.

Lastly, the DT would remind entities that FERC issued Order Nos. 893 and 893-A in 2023, which provide *Incentives for Advanced Cyber security Investment* as directed by the Infrastructure Investment and Jobs Act of 2021. The Order establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the Order as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Gail Golden - Entergy - Entergy Services, Inc. - 5

Answer

Document Name

Comment

Will need to research a solution to see if it is cost effective.

Likes 0

Dislikes 0

Response

Thank you for your comment.

James Keele - Entergy - 3

Answer

Document Name

Comment

Will need to research a solution to see if it is cost effective.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer

Document Name

Comment

Black Hills Corporation will not comment on cost effectiveness.

Likes 0

Dislikes 0

Response

Thank you for your comment.

11. Please provide any additional comments for the DT to consider, if desired.

Patricia Lynch - NRG - NRG Energy, Inc. - 5,6

Answer

Document Name

Comment

none

Likes 0

Dislikes 0

Response

Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments

Answer

Document Name

Comment

PG&E thanks the DT for their consideration of the industry's input which included the creation of CIP-015 and the modifications from the last ballot.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	
<p>Reclamation recommends adding the following definition to the NERC Glossary of Terms:</p> <p>Anomaly - Condition that deviates from expectations based on requirements specifications, design documents, user documents, or standards, or from someone’s perceptions or experiences.</p> <p>Reclamation appreciates the DT’s efforts to incorporate the NIST Framework into the NERC Standards. Reclamation encourages the DT to continue this practice to ensure that NERC standards do not duplicate requirements contained within the NIST Framework.</p>	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT considered whether or not to create a NERC Glossary term for “anomalous.” After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective

1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification

b: marked by incongruity or contradiction : PARADOXICAL

Rachel Schuldt - Black Hills Corporation - 6, Group Name Black Hills Corporation - All Segments

Answer

Document Name

Comment

Black Hills Corporation repeats EEI’s comments: EEI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI’s comments. Generator Owners have been included in Section 4 Applicability. In a [letter order](#) issued on June 24, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," which officially effectuated NERC's transition away from the term "Special Protection System" to the newly-revised term "Remedial Action Scheme (RAS).

Larry Snow - Cogentrix Energy Power Management, LLC - NA - Not Applicable - Texas RE,NPCC,SERC,RF

Answer

Document Name

Comment

Cogentrix recommends a longer comment period for a new standard(s). This compressed comment period does not provide commentors with enough time to adequately assess the proposed language of the standard and could lead inadequate or problematic standards.

Likes 0

Dislikes 0

Response

Thank you for your comment. The Standards Committee approved a waiver in August of 2023 that allowed the DT to post for as few as 20 days for industry comment. An additional waiver was approved by the Standards Committee in February 2024. These waivers were necessary to meet the regulatory deadline of July 2024.

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman

Answer

Document Name

Comment

MPC supports comments submitted by the MRO NERC Standards Review Forum.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to MRO NSRF's comments.

C. A. Campbell - LS Power Development, LLC - 5

Answer

Document Name

Comment

Thank you so much for the opportunity to comment.	
Likes	0
Dislikes	0
Response	
Thank you for your comment.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
Generator Owner was left out of applicability, should be re-added.	
Likes	0
Dislikes	0
Response	
Thank you for your comment. Generator Owners have been included in Section 4 Applicability.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
No additional comments	
Likes	0

Dislikes	0
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	
Document Name	
Comment	
While TVA appreciates the flexibility afforded by the proposed risk-based language, additional clarity or assurance regarding how the CEA will approach auditing and determine sufficiency would be helpful.	
Likes	0
Dislikes	0
Response	
Thank you for your comment.	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE support's EEI's comment(s): EI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).	
Likes	0
Dislikes	0

Response

Thank you for your comment. Generator Owners have been included in Section 4 Applicability. RAS will not be revised to SPS. In a [letter order](#) issued on June 24, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," which officially effectuated NERC's transition away from the term "Special Protection System" to the newly-revised term "Remedial Action Scheme (RAS).

David Jendras Sr - Ameren - Ameren Services - 3

Answer

Document Name

Comment

Ameren agrees with and supports EEI comments.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh

Answer

Document Name

Comment

NST respectfully offers the following comments/suggestions on the Technical Rationale document:

> The document includes several statements about compliance that seem to have been written as statements of fact. Three examples, numbered for reference purposes, are:

(1) "Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and not a cause for potential non-compliance with Requirement R1, Part 1.2 or 1.3."

(2) "Short periods of reduced visibility should not justify a potential non-compliance finding, especially when other cybersecurity monitoring is in place."

(3)"Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2."

NST believes it is beyond the SDT's purview to make such assertions, and we therefore recommend they be reworded to clarify they only represent STD opinions.

With regard to statement (1) and the idea of suspending INMS monitoring or suppressing alerts while maintenance and/or system upgrade activities are in progress, we believe a better approach to allowing an Entity to do this without risking instances of non-compliance would be to add exception language to Requirement R1 that allows for this.

> NST believes the paragraph titled, "External Networks" is confusing at best. We presume the STD's intent is to encourage Entities to implement INSM in high-value networks outside of ESP. While we are inclined to agree it might be worthwhile, we believe that by virtue of being beyond the scope of CIP-015, it should be omitted.

Likes	0
Dislikes	0

Response

Thank you for your comments and for pointing out these statements.

For (1) and (2). We will discuss the addition of a statement such as "it is the opinion of the DT" in those sections.

For (3) the DT intends to specify that an INSM system that provides any form of anomaly detection is a compliant system. This wording and other similar language in the TR is designed to remove ambiguity during audits where the tool selection might be brought into question based on the technology used by the tool. FERC Order No. 887 specifies that the Reliability Requirement be "technology neutral" (Paragraph 77) and this language is included in the TR to ensure that any detection algorithm used by the Responsible Entity is compliant with R1 Part 1.2.

Regarding adding exception language, we've discussed exceptions at length several times and each time concluded that we do not want to increase compliance burden for the Responsible Entities. If we add exception language, then entities must demonstrate compliance to the

exception and spend resources on activity that does nothing to improve reliability or detect threats. Suppressing and tuning of alerts is a common daily activity and does not justify additional CIP paperwork that might come under audit scrutiny.

The “External Networks” paragraph is specifically related to networks where data is shared to and from an ESP, such as ICCP networks, turbine monitoring networks (e.g. GE M&D). We’ve changed the heading to “partner networks” and made significant changes. These networks are very high value, and we want to ensure that the intent is clear.

Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster

Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #11.	
Likes	0
Dislikes	0

Response

Thank you for your comment. Please see responses to EEI’s comments.

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	
Document Name	
Comment	
The NAGF notes that the phrase “detecting anomalous or unauthorized activity” in section R1 is of concern as the use of the word “unauthorized” implies a program to authorize network level activity within the ESP. As a network level monitoring standard, entities will need additional context of system monitoring (such as logs) or other data (e.g., work orders for adding new devices to a network) to determine “unauthorized activity” from a detected anomaly. Also, with an “or” between them, an entity can monitor for only unauthorized	

and ignore anomalous traffic. As unauthorized activity is a subset of anomalous activity, we suggest striking “or unauthorized”. It is also noted that requirement part 1.2 only mentions “anomalous network activity” and this would align it with the remainder of the sub-requirements.

Likes 0

Dislikes 0

Response

Thank you for your comment. The DT revised Requirement R1 and removed “or unauthorized” from the requirement.

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer

Document Name

Comment

Thank you for the opportunity to comment.

Likes 0

Dislikes 0

Response

Thank you for your comment.

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer

Document Name

Comment

Texas RE reiterates its concerns that this standard would be a challenge to audit and enforce consistently. In Requirement R1, the phrase “based on network security risk(s)” is vague and does not include criteria establishing the network security risks, which could lead to Parts 1.2

and 1.3 not being relevant. Second, Requirement R3 does not specify how an entity should determine the retention periods, thus leading to a vague requirement.

Likes 0

Dislikes 0

Response

Thank you for your comment.

For R1, the current draft has the language “Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications”...the DT believes that this will allow entities to customize their monitoring locations and to have a documented rationale for why those locations were chosen for audit defense.

In regard to Requirement R3: The DT has been hesitant thus far to attempt to create a discrete list of timelines for the variety of evidence that would be available to meet the CIP-015 requirements. However, the DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Fong Mua, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Ryder Couch, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Wei Shao, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; - Tim Kelley, Group Name SMUD and BANC

Answer	
Document Name	
Comment	
<p>SMUD recommends the Standards Drafting Team (SDT) change the language in Requirement R1, Part 1.2 so that it is consistent with Requirement R1.</p> <p>Requirement R1 states “Responsible Entity shall implement one or more documented process(es) for internal network security monitoring (INSM) of high impact BES Cyber Systems (BCS) and medium impact BCS with External Routable Connectivity (ERC) within the Responsible Entity’s ESPs to increase the probability of <i>detecting anomalous or unauthorized network activity.</i>”</p> <p>Requirement R1, Part 1.2 states “Implement one or more method(s) to <i>detect anomalous network activity</i> using the data collected at locations identified in Part 1.1.”</p> <p>Although this inconsistency is minor, the SDT has the opportunity to make the change now and improve the quality of this Standard. This language change is non-substantive and could be made for the final ballot posting.</p>	
Likes	0
Dislikes	0
Response	
Thank you for your comment. The DT agrees and revised Requirement R1 and its Parts for consistency and clarity.	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	
Document Name	
Comment	
We support TFIST comments	
Likes	0

Dislikes	0
Response	
Thank you for your comment. Please see responses to TFIST's comments.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	
ATC appreciates the SDT addressing ATC's comments from the previous round while maintaining an objective approach and commensurate flexibility in the requirement language.	
Likes	0
Dislikes	0
Response	
Thank you for your comment.	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	
Document Name	
Comment	
EEI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).	
Likes	0
Dislikes	0
Response	

Thank you for your comment. Generator Owners have been included in Section 4 Applicability. RAS will not be revised to SPS. In a [letter order](#) issued on June 24, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," which officially effectuated NERC's transition away from the term "Special Protection System" to the newly-revised term "Remedial Action Scheme (RAS).

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer

Document Name

Comment

See comments submitted by the Edison Electric Institute

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.

Kinte Whitehead - Exelon - 3

Answer

Document Name

Comment

Exelon is aliging with the EEI in response to this question.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.

Marie Potter - Marie Potter On Behalf of: Alison MacKellar, Constellation, 5, 6; Kimberly Turco, Constellation, 5, 6; - Marie Potter

Answer	
Document Name	
Comment	
Constellation concurs with NAGF's comments. In addition, Constellation wants the DT to provide further guidance on anomalous or for it to be defined.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to NAGF's comments.	
Jodirah Green - ACES Power Marketing - 1,3,4,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name ACES Collaborators	
Answer	
Document Name	
Comment	
ACES would like to thank the SDT for all their hard work and allowing us to provide feedback	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment.	
Hillary Creurer - Allele - Minnesota Power, Inc. - 1	
Answer	
Document Name	

Comment

Minnesota Power supports EEI's comments.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer

Document Name

Comment

OPG supports NPCC Regional Standards Committee's comments:

"NPCC RSC recommends a longer comment period for a new standard(s). This compressed comment period does not provide commentors with enough time to adequately assess the proposed language of the standard and could lead inadequate or problematic standards."

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to NPCC RSC's comments.

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo

Answer

Document Name

Comment

ITC supports EEI's comments on this project.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.

Daniel Gacek - Exelon - 1

Answer

Document Name

Comment

Exelon supports the comments submitted by the EEI for this question.

Likes 0

Dislikes 0

Response

Thank you for your comment. Please see responses to EEI's comments.

Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez

Answer

Document Name

Comment

The Technical rational is well written with a lot of detail, however this document from my understanding will not be part of the audit. I would like to see more in the measures, as a high-level for better understanding. Leaving it up to the entities, may still become audit bait, unless

each entity writes up their rational. The standard is written a Subjective standard vs. an objective standard, this leaves it up to the entity to decide what to audit it on.

The definition anomalous activity needs to be defined; Baseline needs to be defined. Overall, there needs to be a standardized approach for auditing this requirement.

Likes 0

Dislikes 0

Response

Thank you for your comments. The DT considered whether or not to create a NERC Glossary term for “anomalous.” After reviewing the Merriam-Webster dictionary definition, the DT felt “anomalous” adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary.

Anomalous - adjective

1: inconsistent with or deviating from what is usual, normal, or expected : IRREGULAR, UNUSUAL

Example - Researchers could not explain the anomalous test results.

2 a: of uncertain nature or classification

b: marked by incongruity or contradiction : PARADOXICAL

Many vendors use the term “anomaly detection” to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity’s collected traffic. Incoming traffic is then compared to that representation of expected traffic, and this becomes the baseline that incoming traffic is then compared to determine if any traffic is anomalous or not.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

The current technology landscape has a number of vendors which, in many cases, have developed proprietary methods to detect anomalous network behavior. As a result in technology advancements, new anomalous detection products are likely to be introduced.

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI

Answer	
Document Name	
Comment	
<p>The VSLs are too high for R2/R3 compared to R1. Maintaining full logs that only went back 82 days (vs 90) is potentially as or more severe than having a program in place at all (R1). The drafting team should consider a higher VSL for R1 as compared to a lower VSL for R2 & R3 as currently written.</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. The DT considered your comment, but decided to make no change to the VSLs.</p>	
<p>Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable</p>	
Answer	
Document Name	
Comment	
<p>EEI requests a review of the Section 4 Applicability due to the exclusion of Generator Owners in the current proposed draft Standard. In addition, please review 4.2.1.2 as it refers to Special Protection Systems (SPS), not Remedial Action Schemes (RAS).</p>	
Likes	0
Dislikes	0
Response	
<p>Thank you for your comment. Generator Owners have been included in Section 4 Applicability. RAS will not be revised to SPS. In a letter order issued on June 24, 2016, FERC approved the NERC Glossary definition for "Special Protection System (SPS)," which officially effectuated NERC's transition away from the term "Special Protection System" to the newly-revised term "Remedial Action Scheme (RAS).</p>	

Kelly Bertholet – Manitoba Hydro

Question 1 -Yes

Comments: Manitoba Hydro supports this change as the previous conditional inclusions were a source of confusion for many.

Response: Thank you for your support.

Question 2 -Yes

Response: Thank you for your support.

Question 3 -Yes

Comments: Manitoba Hydro supports this clear direction.

Response: Thank you for your support.

Question 4 -Yes

Response: Thank you for your support.

Question 5 -Yes

Comments: Manitoba Hydro agrees with this approach, which is clear in its intent. However, there is a concern that the phrase “detecting anomalous or unauthorized network activity” in R1 does not align well with Parts 1.2 and 1.3. We recommend striking “or unauthorized” in R1 to better align with the rest of the standard and avoid confusion as to whether this criteria is “one or the other” or referring to detecting both anomalous and unauthorized network activity. As unauthorized network activity would also be anomalous, nothing would be lost with its omission.

Response: Thank you for your support. The DT has removed “or unauthorized” and has revised Requirement R1 and its Parts for clarity and consistency.

Question 6 -Yes

Response: Thank you for your support.

Question 7 -Yes

Response: Thank you for your support.

Question 8 -No

Comments: Manitoba Hydro is concerned with the current language in R3. The amount of data needing to be collected and stored just for an audit cycle could be extremely voluminous and overly expensive. Manitoba Hydro believes that the data to be retained should be limited to network communications and other related data that is part of an investigated alert. Full capture of network and other related communications data would be an administrative and a cost burden without providing any additional security or reliability to the Bulk Electric System.

To achieve the retention of meaningful INSM Data and to eliminate the administrative and economic burdens of retaining unmeaningful INSM data, Manitoba Hydro suggests modifying R3:Responsible Entity shall implement one or more documented process(es) to retain meta data collected to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.

Response: Thank you for your support. The DT has made the following change that we believe will hopefully address the concern listed.

Requirement R3 has been revised to the following:

Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3. [Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]

Note: The Responsible Entity is not required to retain detailed INSM data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Question 9 -Yes

Response: Thank you for your support.

Question 10 -Yes

Response: Thank you for your support.

Question 11 – Comments: Generator Owner was left out of applicability, should be re-added.

Response: Thank you for your comment. Generator Owners have been included in Section 4 Applicability.