NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

,

Consideration of Comments

Project Name:	2023-03 Internal Network Security Monitoring | Draft 2 of CIP-015-1
Comment Period Start Date:	4/5/2024
Comment Period End Date:	4/17/2024
Associated Ballot(s):	2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 AB 2 ST 2023-03 Internal Network Security Monitoring (INSM) CIP-015-1 Non-Binding Poll AB 2 NB 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan AB 2 OT

There were 55 sets of responses, including comments from approximately 142 different people from approximately 87 companies representing 10 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

****Please Note: Based on Comments received, the DT reversed the order of Requirements R2 and R3 to better align the order of the requirements. The redline of proposed Reliability Standard CIP-015-1 is reflective of that change. However, the DT found that it was difficult to distinguish the changes in the requirements and measures from the redlines due to re-ordering, so the DT made the re-ordering changes in green text, while the edits in the requirements and measures remain in redline.**

These minimal, non-substantive edits to Requirements R2 (previously R3) and R3 (previously R2) are:

- **R2 (previously R3):** Each 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 Requirement R1, 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~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

- **Measure M2 (Previously M3):** Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.
- **R3 (previously R2):** Each 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~~ R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*
- **Measure M3 (previously M2):** Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

1. Generator Owner was added as 4.1.4. to the Applicability Section. Generator Owner was included in Project 2023-03's SAR. In addition, Generator Owner was included in the revisions to CIP-007 during the initial posting of Project 2023-03, INSM, but was inadvertently left out of the initial posting of proposed Reliability Standard CIP-015-1 (additional posting for the project). Do you support updating proposed Reliability Standard CIP-015-1 to include Generator Owner in 4.1.4. of the Applicability Section? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

The DT received supportive comments for adding the Generator Owner to 4.1.4. of the Applicability Section.

2. Based on industry feedback, Requirement R1 and its Parts and Measure M1 were revised for consistency and clarity. Do you agree with the language proposed in Requirement R1 and its Parts and Measure M1? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

For Requirements R1, R2 and R3, the DT added the word "Each" at the beginning of the requirements to align with the CIP family of standards.

The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system. 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)."

Each entity is expected to develop an INSM system that continuously compares incoming traffic to its established baseline of expected network traffic to detect anomalous network activity. However, the drafting team envisioned scenarios where an entity would want to pause monitoring for a period of time (during equipment maintenance or replacement) or INSM equipment could fail, and continuous monitoring be interrupted. The DT did not want entities to be subject to a potential finding of non-compliance during these scenarios and thus did not specify continuous monitoring in the requirements.

The DT considered whether or not to create a NERC Glossary term for “anomalous”. The Merriam-Webster dictionary defined anomalous as:

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 addresses this in the FAQ document, and has provided some updates to the Technical Rationale document for additional clarity.

The DT did not add CIP Exceptional Circumstance to Requirement R1 because it was determined that once an entity has established and documented their process and methods for performing INSM in their ESP networks, a CIP Exceptional Circumstance should not materially impact their INSM program from the perspective that the equipment would already be installed, and a detection and evaluation process has already been implemented. While continuous monitoring is the goal of the standard, the DT did not include a continuous monitoring requirement to allow for situations where an entity has an equipment failure, needs to perform maintenance that would interrupt monitoring, or determines that the INSM system should be shut down for a period of time to perform generation plant or substation maintenance. The risk-based rationale should be used to describe why an entity chose not to monitor specific ESP networks if they choose not to monitor the entirety of their ESP networks. Examples are provided in the Technical Rationale and FAQ to describe how those risk-based decisions could be made. The DT believes that including “risk-based rationale” is more encompassing than alternative language proposed by several commenters.

3. Based on industry feedback, Requirement R2 and Measure M2 were revised to clarify that: retained INSM data needs to be protected. Do you agree with the language proposed in Requirement R2 and Measure M2? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

***Based on Comments received, the DT reversed the order of Requirements R2 and R3 to better align the order of the requirements. The redline of proposed Reliability Standard CIP-015-1 is reflective of that change. However, the DT found that it was difficult to distinguish the changes in the requirements and measures from the redlines due to re-ordering, so the DT made the re-ordering changes in green text, while the edits in the requirements and measures remain in redline.**

These minimal, non-substantive edits to Requirements R2 (previously R3) and R3 (previously R2) are:

- **R2 (previously R3):** Each 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 Requirement R1, 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~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

- **Measure M2 (Previously M3):** Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.

- **R3 (previously R2):** Each 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~~ R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

- **Measure M3 (previously M2):** Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

The intent of Requirement R3 (previously R2) is to protect the collected INSM data from modification or deletion by an adversary. The Technical Rationale has been updated to read: “The Responsible Entity’s existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

The intent of Requirement R3 (previously Requirement R2) is to protect the collected INSM data from modification or deletion by an adversary.

4. Based on industry feedback, Requirement R3 and Measure M3 were revised for clarity of data retention requirements and a note following Requirement R3 was added to ensure that there is an explicit statement about not requiring the retention of data that is not relevant to anomaly network activity detected. Do you agree with the language proposed in Requirement R3 and Measure M3? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Summary Response:

***Based on Comments received, the DT reversed the order of Requirements R2 and R3 to better align the order of the requirements. The redline of proposed Reliability Standard CIP-015-1 is reflective of that change. However, the DT found that it was difficult to distinguish the actual changes in the requirements and measure from the redlines due to re-ordering, so the DT made the re-ordering changes in green text, while the edits in the requirements and measures remain in redline.**

These minimal, non-substantive edits to Requirements R2 (previously R3) and R3 (previously R2) are:

- **R2 (previously R3):** Each 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 Requirement R1, 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~~ internal network security monitoring data ~~(full packet capture data, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.
- **Measure M2 (Previously M3):** Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.
- **R3 (previously R2):** Each 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~~ R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

- **Measure M3 (previously M2):** Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.

In response to commenters, the DT updated the Note in Requirement R2 (previous Requirement R3) to “Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture date, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2,” to clarify the intent of the Note. The word “detailed” was removed, as information would not be required to be retained that is not relevant to the anomalous activity.

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

Summary Response:

Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.

The Technical Rationale has been updated to read: ~~The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing[1]”~~ The Responsible Entity’s existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

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 DT considered whether or not to create a NERC Glossary term for “anomalous.” The Merriam-Webster dictionary defined anomalous as:

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.

The INSM system may be classified as BCSI or EACMS per the existing processes for each entity.

Changes to requirements and compliance solutions of CIP-004, CIP-005, CIP-007, and CIP-010 are outside of the scope of Project 2023-03.

The DT provided an implementation timeframe of 36 months for high impact and medium impact control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the 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.

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
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
Jay Sethi	Jay Sethi		MRO	Manitoba Hydro Group	Nazra Gladu	Manitoba Hydro	1	MRO
					Mike Smith	Manitoba Hydro	3	MRO

					Kristy-Lee Young	Manitoba Hydro	5	MRO
					Kelly Bertholet	Manitoba Hydro	6	MRO
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 -	1	SERC

						Southern Company Services, Inc.		
					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
					Ryan Strom	Buckeye Power, Inc.	4	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Colette Caudill	East Kentucky Power Cooperative	1	SERC
					Tony Kroskey	Brazos Electric Power	1	Texas RE

						Cooperative, Inc.		
					Katrina Lyons	Georgia System Operations Corporation	4	SERC
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Bill Pezalla	Old Dominion Electric Cooperative	3,4	SERC
					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
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
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Randy Buswell	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC
					Dermot Smyth	Con Ed - Consolidated	1	NPCC

						Edison Co. of New York		
					David Burke	Orange and Rockland	3	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					David Kwan	Ontario Power Generation	4	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
					Sean Cavote	PSEG	4	NPCC
					Jason Chandler	Con Edison	5	NPCC
					Tracy MacNicoll	Utility Services	5	NPCC

Shivaz Chopra	New York Power Authority	6	NPCC
Vijay Puran	New York State Department of Public Service	6	NPCC
David Kiguel	Independent	7	NPCC
Joel Charlebois	AESI	7	NPCC
Joshua London	Eversource Energy	1	NPCC
Emma Halilovic	Hydro One Networks, Inc.	1,2	NPCC
Emma Halilovic	Hydro One Networks, Inc.	1,2	NPCC
Chantal Mazza	Hydro Quebec	1,2	NPCC
Emma Halilovic	Hydro One Networks, Inc.	1,2	NPCC
Chantal Mazza	Hydro Quebec	1,2	NPCC
Nicolas Turcotte	Hydro-Quebec (HQ)	1	NPCC

					Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
					Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
					Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
					Joel Charlebois	AESI	7	NPCC
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

1. Generator Owner was added as 4.1.4. to the Applicability Section. Generator Owner was included in Project 2023-03's SAR. In addition, Generator Owner was included in the revisions to CIP-007 during the initial posting of Project 2023-03, INSM, but was inadvertently left out of the initial posting of proposed Reliability Standard CIP-015-1 (additional posting for the project). Do you support updating proposed Reliability Standard CIP-015-1 to include Generator Owner in 4.1.4. of the Applicability Section? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
No additional comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE agrees with EEI comments: EEI agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.	
Likes 0	
Dislikes 0	

Response	
Thank you for your support. Please see responses to EEI’s comments.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
We support EEI's comments: EEI agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.	
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.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with the addition of Generator Owners to the Applicability Section of CIP-015-1.	
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	

Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports adding Generator Owner to the Applicability Section of the proposed CIP-015-1.	
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 agrees with the comments submitted by EEI.	
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 and NAGF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s and NAGF’s comments.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this questions in alignment with the EEI.	
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 responding to this question in alignment with the EEI.	
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	
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.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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.	
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.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
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.	
James Keele - Entergy - 3	
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.	
Tyler Schwendiman - ReliabilityFirst - 10	
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.	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	Yes
Document Name	
Comment	
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	
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.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung 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.	
Roger Perkins - Southern Maryland Electric Cooperative - 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.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan	
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.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
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.	
Ben Hammer - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 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.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
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.	

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
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.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
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.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
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.	

2. Based on industry feedback, Requirement R1 and its Parts and Measure M1 were revised for consistency and clarity. Do you agree with the language proposed in Requirement R1 and its Parts and Measure M1? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments: "We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection. Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement. Please clarify the term BES Security systems."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to NPCC RSC’s comments.	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	

Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc., so that the utilities can have a standardized method to determine **in-scope high and medium impact BCS with ERC**.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system.

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 disagrees with the proposed revision to Requirement R1 as it still has no guidance as to if detection is to be continuous or periodic. In addition, there is still no timeline as to how often detection and evaluation are to be performed. What if the technology is not available, and a RE wants to do this manually? Can the RE say they checked a tool once a year, such as wireshark, at a planned interval and call it compliant?

SRP is still unclear on what an auditor would look for evidence to meet this requirement. Would system logs, alert screens, email generated alerts, or others be acceptable evidence? Also, there needs to be guidance or a definition of a network communication baseline. This has yet been defined. The technical guidelines, provides an example of a baseline. However, the methods still do not call out what a baseline consists of. This needs to be included in the Methods of examples of what may be included in a baseline.

Likes 0	

Dislikes 0	
Response	
Thank you for your comments. Each entity is expected to develop an INSM system that continuously compares incoming traffic to its established baseline of expected network traffic to detect anomalous network activity. However, the drafting team envisioned scenarios where an entity would want to pause monitoring for a period of time (during equipment maintenance or replacement) or INSM equipment could fail and continuous monitoring be interrupted. The DT did not want entities to be subject to a potential finding of non-compliance during these scenarios and thus did not specify continuous monitoring in the requirements. The scenario you suggest would not be an acceptable method to meet the requirements, however. Depending on the INSM tools the entity selects, the baseline could be created using different vendor proprietary methods. Given that there is not a single method of developing a baseline that could apply to all vendor products and future INSM solutions using new tools such as AI, the DT chose not to provide specifics in Requirement R1 for how to develop a baseline. Section C of the standard provides information on evidence retention.	
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 believes using the phrase “Implement, using a risk-based rationale” without establishing minimal criteria could create a modification to the standard before it becomes effective. FERC has not approved of the ERO’s risk-based approaches in the past when there is no minimum requirement/rationale/criteria to be considered and has often required additional modifications to standards and requirements due to this approach. ACES believes a better approach would be to start with minimum criterion for entities to consider from a risk-based perspective. Furthermore, ACES questions whether internal network security monitoring provides additional security or reduces the risk to the BES. For the Responsible Entity to be able to detect anomalous activity within its ESP, it must first be able to analyze all traffic on all networks within the ESP. If, through the application of best practice network design, an entity has chosen to implement additional security by significantly segmenting their network(s), the entity must a) expend a significant amount of capital to install additional monitoring equipment or b) reduce its overall security posture by flattening its networks to comply with the proposed language of Requirement R1. As technology advances, so does security. ACES has observed this progression as the use of encryption in IP-based protocols becomes more prevalent. Those who wish to threaten the BES understand these principles and will continue to utilize them to disguise nefarious traffic,	

thereby going undetected by INSM. Over time, as the practice of encrypting network traffic while in transit becomes more widespread, utilizing INSM to detect potential intrusion(s) and/or anomalous network traffic will make it a less effective tool than it is currently.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.

The DT notes that many encrypted protocols (including HTTPS) are not fully encrypted, which allows INSM systems to monitor important information, such as certificates and user-agent strings. We note that collecting this data allows entities to detect and alert on several attack techniques even for protocols with bolted on transport layer security encryption. Last, many SCADA systems require the use of active directory or similar directories, server message block and similar file transfer systems which encrypt portions of payloads, but not all of the payload. An INSM system can carve files from these protocols, including active directory group policy settings.

Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

R1, Part 1.1: SPP respectfully asks the SDT to consider a “per system capability” clause due to potential technology limitations for entities (future technologies).

R1, Part 1.3: 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 comments. The DT determined that INSM should be capable of being installed, at least in some fashion, in any of an entity’s ESP networks. INSM technologies have been developed specifically to be installed in operational technology (OT) environments as a passive detection mechanism and detect anomalous behavior in most modern OT protocols. Duplication of network traffic can be accomplished through the use of hardware network taps, which were invented in 2000, or switch port mirroring (Cisco calls this SPAN) available on commercial and industrial network switches for over the past 10 years. The DT disagreed with your suggestion to change “to” to “and,” as doing so would create a requirement for two activities. The DT intended the evaluation to lead entities to a conclusion on what action they should take. Those actions could be determining the anomalous network traffic is a legitimate and benign false positive, is abnormal but not malicious perhaps requiring a configuration change, or potentially malicious and needs to be escalated to your CIP-008 process for handling as a possible cybersecurity incident or attempt to compromise.	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc. so that the utilities can have a standardize method to determine **in-scope high and medium impact BCS with ERC**.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.	
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 comments. Please see responses to ISO/RTO IRC’s comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	
We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection. Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement. Please clarify the term BES Security systems.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system. 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).” “BES Security Systems” was an error in the redline document, which was updated and reposted during the comment period. The term was intended to be “BES Cyber Systems.” This was reflected correctly in the clean version of the document.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	
Comment	
We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection. Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement. Please clarify the term BES Security systems.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.

“BES Security Systems” was an error in the redline document, which was updated and reposted during the comment period. The term was intended to be “BES Cyber Systems.” This was reflected correctly in the clean version of the document.

Ben Hammer - Western Area Power Administration - 1,6

Answer	No
Document Name	

Comment

The standards drafting committee needs develop NERC defined terms and definitions for the following terms:

- Anomalous Network activity
- Network Data Feeds

The standards drafting committed needs to address wither the INSM systems constitutes an EACM(S) and or BCSI repository or both.

The drafting team needs to provide a reasonable compliance solution, acceptance of work of others, or changes to the requirements in CIP-004, CIP-005, CIP-007, and CIP-010 to assist Responsible Entities (REs) with the ability to maintain compliance for cloud-based solutions for INSM.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT considered whether or not to create a NERC Glossary term for “anomalous”. The Merriam-Webster dictionary defined anomalous as:

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.

The Responsible Entity’s existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

Changes to requirements and compliance solutions of CIP-004, CIP-005, CIP-007, and CIP-010 is outside of the scope of Project 2023-03.

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

Answer	No
Document Name	

Comment

R1

The ISO/RTO Council (IRC) Standards Review Committee (SRC) is concerned that requirement R1, unlike requirements R2 and R3, does not include language such as, or is similar to, *“except during CIP Exceptional Circumstances”*. The Technical Rationale includes a discussion on “*Aligning Collection and Monitoring with Operations”* (p. 8) where it describes situations where *“Operational changes might require temporary or extended removal of INSM collection capability at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and, in the opinion of the DT, does not constitute cause for non-compliance with Requirement R1, Part 1.2. or 1.3.”* While the SRC agrees with the Technical Rationale, the Technical Rationale is not enforceable. The SRC suggests that language such as, or similar to, the following be included within the requirement to establish clarity and encourage consistency in auditing practices:

Except during CIP Exceptional Circumstances or when Operational changes might require temporary or extended removal of INSM collection capability at specific locations.

R1.1

The SRC recommends that the standard be revised to clarify the intended meaning of “*risk-based rationale*.*”* While the concept of “rationale” is well understood, it may be beneficial to create a sub-requirement (such as 1.1.1) where the term risk-based is clearly defined in such a way that encourages consistent audit practices. For example, in FAC-003-5 Transmission Vegetation Management, the Background section includes the following to describe the concept of risk-based:

“Risk-based preventive requirements to reduce the risks of failure to acceptable tolerance levels. A risk-based reliability requirement should be framed as: who, under what conditions (if any), shall perform what action, to achieve what particular result or outcome that reduces a stated risk to the reliability of the bulk power system?”

The SRC is also concerned that the term “feed(s)” is not clear and could be misconstrued to not require collection of data. The SRC suggests that the term “feed(s)” be replaced with the term “collection point(s)”. The SRC recommends the following revision:

1.1. Implement, using a risk-based rationale, network data collection points to monitor network activity; including connections, devices, and network communications.

The related language in M1 Part 1.1 should also be revised to reflect this change.

R1.2

The SRC proposes that the phrase “network data feed(s)” be replaced with “network data collection point(s)” to ensure consistency with R1.1 as indicated in the previous comment. The SRC recommends the following revision:

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

M1

The SRC is concerned that M1 includes the language “Evidence must include”. This is inconsistent with most, if not all, of the NERC CIP standards and specifically with M2 and M3 of this standard, which state “Evidence may include”. The SRC recommends that the language in M1 be revised to be consistent with M2 and M3.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT did not add CIP Exceptional Circumstance to Requirement R1 because it was determined that once an entity has established and documented their process and methods for performing INSM in their ESP networks a CIP Exceptional Circumstance should not materially impact their INSM program from the perspective that the equipment would already be installed and a detection and evaluation process has already been implemented. While continuous monitoring is the goal of the standard, the DT did not include a continuous monitoring requirement to allow for situations where an entity has an equipment failure, needs to perform maintenance that would interrupt monitoring, or determines that the INSM system should be shut down for a period of time to perform generation plant or substation maintenance. The risk-based rationale should be used to describe why an entity chose not to monitor specific ESP networks if they choose not to monitor the entirety of their ESP networks. Examples are provided in the Technical Rationale and FAQ to describe how those risk-based decisions could be made. The DT believes that including “risk-based rationale” is more encompassing than alternative language proposed by several commenters.

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).” Using the associated measure, the Responsible Entity can document the risk-based rationale that describes how network data feed(s) were selected.

Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza

Answer	No
Document Name	

Comment

We think some focus needs to go into driving consistency between R1, R2, and R3. Methods vs Processes and Feeds vs Collected/Collection.

Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement.

Please clarify the term BES Security systems.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.

“BES Security Systems” was an error in the redline document, which was updated and reposted during the comment period. The term was intended to be “BES Cyber Systems.” This was reflected correctly in the clean version of the document.

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

Answer	No
Document Name	

Comment

NST appreciates that the SDT has tried to avoid being overly prescriptive. However, we believe that requiring entities to use a "risk-based rationale" to designing and implementing INSM is (a) unnecessary - an entity either has or hasn't implemented INSM in a manner that covers all BES Cyber Systems within an ESP, and (b) could result in endless arguments among Responsible Entities, Regions, and NERC over what might be considered acceptable approaches to establishing a risk-based rationale for implementation choices.

NST suggests not using the phrase, "network data feeds," as the term, "data feeds" is widely used to describe data made available to users, typically via web servers, that provides real-time information about road conditions, weather, stock indices, etc.

NST recommends revising R1 Part 1.1 to simply state, "Identify network data collection methods and locations, which may be either physical or virtual, used to monitor network activity including connections, devices, and network communications."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT recognizes 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. The risk-based rationale should be used to describe why an entity chose not to monitor specific ESP networks if they choose not to monitor the entirety of their ESP networks. Examples are provided in the Technical Rationale and FAQ to describe how those risk-based decisions could be made. The DT believes that including “risk-based rationale” is more encompassing than alternative language proposed by several commenters. 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. The DT reviewed your comment but decided Requirement R1, Part 1.1 is written as intended, so made no change.	
Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan	
Answer	No
Document Name	
Comment	
Is this risk is based on reliability only or other things as well? More details need to be provided. Not sure what is required in content in rationale. Without having a requirement on the content of the rationale it is subject to interpretation depending on the risk methodology expected. Risk based rationale should be its own requirement.	
Likes 0	

Dislikes 0	
Response	
Thank you for your comments. The DT recognizes 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. The risk-based rationale should be used to describe why an entity chose not to monitor specific ESP networks if they choose not to monitor the entirety of their ESP networks. Examples are provided in the Technical Rationale and FAQ to describe how those risk-based decisions could be made. The DT believes that including “risk-based rationale” is more encompassing than alternative language proposed by several commenters. 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.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	No
Document Name	
Comment	
SMECO agrees with ACES comments: ACES believes using the phrase “Implement, using a risk-based rationale” without establishing minimal {C}[A1]{C} criteria could create a modification to the standard before it actually becomes effective. FERC has not approved of the ERO’s risk-based approaches in the past when there is no minimum requirement/rationale/criteria to be considered and has often required additional modifications to standards and requirements due to this approach. ACES believes a better approach would be to start with minimum criterion for entities to consider from a risk-based perspective. Furthermore, ACES questions whether internal network security monitoring provides additional security or reduces the risk to the BES. For the Responsible Entity to be able to detect anomalous activity within its ESP, it must first be able to analyze all traffic on all networks within the ESP. If, through the application of best practice network design, an entity has chosen to implement additional security by significantly segmenting their network(s), the entity must a) expend a significant amount of capital to install additional monitoring equipment or b) reduce its overall security posture by flattening its networks to comply with the proposed language of Requirement R1.	

As technology advances, so does security. ACES has observed this progression as the use of encryption in IP-based protocols becomes more prevalent. Those who wish to threaten the BES understand these principles and will continue to utilize them to disguise nefarious traffic, thereby going undetected by INSM. Over time, as the practice of encrypting network traffic while in transit becomes more widespread, utilizing INSM to detect potential intrusion(s) and/or anomalous network traffic will make it a less effective tool than it is currently.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to ACES's comments.	
Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung 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 appreciates the efforts of the Standards Drafting Team (SDT) in responding to the industry's comments on the initial draft and proposing these new revisions so quickly. In Requirement R1 Part 1.1, instead of using the words "network data feeds" we prefer the original wording of "data collection locations", or alternately "data collection sources" because the wording of "data collection feeds" could be interpreted as a *subscription* to threat/intelligence feeds.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 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)."	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro appreciates the drafting team efforts to address our comments in Draft 1. However, BC Hydro has the following comments on Draft 2. The use of the 'risk-based rationale' 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. 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. BC Hydro also 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. 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 comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system.

The DT considered whether or not to create a NERC Glossary term for "anomalous". The Merriam-Webster dictionary defined anomalous as:

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 updated the Technical Rationale document for additional clarity.

James Keele - Entergy - 3

Answer	No
Document Name	

Comment

For R1.2, 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 comments. The DT considered whether or not to create a NERC Glossary term for “anomalous”. The Merriam-Webster dictionary defined anomalous as:

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 updated the Technical Rationale document for additional clarity.

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

Answer	No
Document Name	

Comment

BPA believes that adding the phrase “using a risk-based rationale” reduces but does not eliminate ambiguity about the requirement. Ambiguity opens REs to subjective criticism from auditors. Therefore, BPA still recommends adding language used elsewhere in the CIP Standards, specifically “as determined by the Registered Entity”, to strengthen the position that the REs are empowered to set their own risk-based rationale.

BPA supports discontinuing the term “locations” in R1. However, not every RE will refer to the two books cited in the Technical Rationale to develop an understanding of the newly proposed term “network data feed”. The Technical Rationale provides a lengthy, complex explanation of the intent of the term. BPA requests that the SDT include a brief, simple, clear definition in addition to the three paragraphs of explanation.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity’s environment when they develop an INSM system.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	2023-03 Unofficial_Comment_Form_April 2024 NSRF.docx
Comment	
MRO NSRF thanks the drafting team for an excellent job in addressing stakeholder comments and adjusting the standard language. For R1, R2 and R3 we suggest beginning each with either “The” or “Each” to match CIP-002, CIP-012 and CIP-013. The following non-substantive changes are suggested to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”: **The/Each** 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. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity **and** shall include each of the following requirement Parts:	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. For Requirements R1, R2, and R3, the DT added the word “Each” at the beginning of the requirements to align with the CIP family of standards. The suggested clarity revision was not made because the DT believes Requirement R1 is clear as written.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes

Document Name	
Comment	
Ameren agrees with and supports EEI and NAGF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's and NAGF's comments.	
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 comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. 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	Yes
Document Name	
Comment	

Evergy supports and incorporates the comments of the Edison Electric Institute (EEI) for Question #2 regarding potential non-substantive changes the drafting team could make to R1, R2, and R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language for CIP-015-1 Requirement R1 and Measurement M1.	
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	
Duke Energy supports EEI comments.	

Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1.	
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 revisions made by the Standard Drafting Team to clarify Requirement R1. While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team's consideration:We suggest adding the word "The" or "Each" to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013.	

Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”: “**The/Each** 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. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity **and** shall include each of the following requirement Parts:”	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. For Requirements R1, R2, and R3, the DT added the word “Each” at the beginning of the requirements to align with the CIP family of standards. The suggested clarity revision was not made because the DT believes Requirement R1 is clear as written.	
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.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	

Comment

We support EEI's comments:

EEI agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1.

While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team’s consideration:

We suggest adding the word “The” or “Each” to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013.

Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”:

“**The/Each** 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. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity **and** shall include each of the following requirement Parts:”

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 agrees with EEI comments: EEI agrees with the revisions made by the Standard Drafting Team to clarify Requirement R1.

While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team’s consideration:

We suggest adding the word “The” or “Each” to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013. Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”: “**The/Each** 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. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity. The documented process(es) **and** shall include each of the following requirement Parts:”	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments.	
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: While the language as written is sufficient, we have provided non-substantive, clarifying edits for the drafting team’s consideration: • We suggest adding the word “The” or “Each” to the beginning of Requirements R1, R2, and R3 to match CIP-002, CIP-012 and CIP-013. • Specific to Requirement R1, the following non-substantive edits provide below are meant to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence “provide methods for…”:	

"**The/Each** 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 (*remove: "to")*. **The documented process(es) shall** provide methods for detecting and evaluating anomalous network activity. *(remove: "The documented process(es)")* **and** shall include each of the following requirement Parts:"	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
The updated language to R1 implies that the Responsible Entity would be implementing data feeds into their environment to monitor network activity. The intent of this requirement is to identify which data feeds within the environment the Responsible Entity will be monitoring network activity. We would suggest removing "implement" and reinstating "identify".	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT previously used "identify" and commenters suggested that language was not clear, so the DT made the change to "implement."	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	

Comment	
FirstEnergy requests that the Regulating Body has determined an INSM as applicable to CIP-015. Until this is clear, there could be various interpretations for compliance. Understanding this interpretation will be a challenge for all to come to a conclusion of a baseline and must come to a consensus based on individual interpretation.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
The standard drafting team has done an excellent job in addressing stakeholder comments and adjusting the standard language. For R1, R2 and R3 MH suggests beginning each with either "The" or "Each" to match CIP-002, CIP-012 and CIP-013. This is a non-substantive change. The following non-substantive changes are suggested to improve the clarity of the requirement in terms of the subject of the verb in the part of the sentence "provide methods for…": The/Each 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. The documented process(es) shall provide methods for detecting and evaluating anomalous network activity and shall include each of the following requirement Parts:	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. For Requirements R1, R2, and R3, the DT added the word “Each” at the beginning of the requirements to align with the CIP family of standards.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
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.	
Ruchi Shah - AES - AES Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 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.	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
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.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
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.	
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.	
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.	
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	
Document Name	
Comment	
Texas RE appreciates the SDT’s consideration if previous comments submitted. In order to clarify and ensure the measures and requirement language are aligned, Texas RE recommends adding “documented” in front of risk-based rationale in Requirement Part 1.1: 1.1 Implement, using a *documented* risk-based rationale, network data feed(s)…	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Requirement R1 already includes a requirement to “implement one or more documented process(es)” and those "processes shall include each of the following requirement Parts:” Thus the drafting team felt that the risk-based rationale used in Requirement R1, Part 1.1 already requires documentation as part of an entity’s INSM process.	

3. Based on industry feedback, Requirement R2 and Measure M2 were revised to clarify that: retained INSM data needs to be protected. Do you agree with the language proposed in Requirement R2 and Measure M2? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA recommends adjusting the wording of R2 to eliminate confusing grammar: “Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to mitigate the risks of unauthorized deletion or modification of internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R3.”	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT modified the language based on previous comments on a prior draft of CIP-015-1. The DT believes that the current grammar is still appropriate.	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro appreciates the drafting team efforts to address our comments in Draft 1. However, BC Hydro has the following comments on Draft 2.	

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 comments. The intent of Requirement R2 is to protect the collected INSM data from modification or deletion by an adversary. The Technical Rationale has been updated to read: “The Responsible Entity’s existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.”

Tim Kelley - Tim Kelley On Behalf of: Charles Norton, Sacramento Municipal Utility District, 3, 6, 4, 1, 5; Foung 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 recommends the Standards Drafting Team swap Requirements R2 and R3 to better align the requirements in the order they should be implemented.

Requirement R2 is to “protect” INSM data against unauthorized deletion in support of Requirement R3. Requirement R3 is to “retain” INSM data associated with network activity determined to be anomalous. The methods to “detect” anomalous network activity should be addressed *before* methods to “protect” INSM data against unauthorized deletion. Therefore, we recommend moving R2 to R3, and R3 to R2. We feel that this change would be non-substantive and could be made in the final ballot.

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	No
Document Name	
Comment	
SMECO agrees with ACES comments: While the requirement essentially says the same thing, ACES believes more cyber security-focused and known terms should be used: "….to mitigate the risks to the confidentiality, integrity, and availability of the collected data."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to ACES's comments.	
Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan	
Answer	No
Document Name	
Comment	

More clarity is required on which data needs to be protected. What is meant by protection method (mitigation of unauthorized modification)?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Technical Rationale provides additional insights for this. The intent of Requirement R3 (previously Requirement R2) is to protect the collected INSM data from modification or deletion by an adversary. Compliance with this requirement includes implementation of protective and detective controls.	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
NST recommends that R2 address the protection of collected INSM data both in storage and in transit (e.g., from a substation with medium impact BCS with ERC to a SIEM system located at an entity's headquarters or a Control Center).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT discussed your comment, but did not want to be that prescriptive.	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	No
Document Name	
Comment	

R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT clarified in Requirement R3 (previously Requirement R2) what data needed to be protected in the previous draft, Technical Rationale, and FAQ.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	
Comment	
R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT clarified in Requirement R3 (previously Requirement R2) what data needed to be protected in previous draft, Technical Rationale, and FAQ.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	

R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT clarified in Requirement R3 (previously Requirement R2) what data needed to be protected in previous draft, Technical Rationale, and FAQ.	
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	
While the requirement essentially says the same thing, ACES believes more cyber security-focused and known terms should be used: "….to mitigate the risks to the confidentiality, integrity, and availability of the collected data."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Technical Rationale provides additional insights for this. The intent of Requirement R3 (previously Requirement R2) is to protect the collected INSM data from modification or deletion by an adversary. Compliance with this requirement includes implementation of protective and detective controls.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No

Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments: "R1 no longer requires collected data, it requires monitoring of feeds of network activity. Include specification of alerting based on network anomaly analysis as source of data that needs protection."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to NPCC RSC’s comments.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
The wording of requirement R2 and M2 clearly outline the requirements. A non-substantive change is suggested to re-order R2 and R3, so that a future requirement is not referenced. This will make it easier to read the standard in order. If this is adopted, then references to R3 would become R2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
No additional comment.	
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 revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
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 agrees with EEI comments: EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
We support EEI's comments: EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
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.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	

Avista agrees with the revisions to Requirement R2 and Measure M2. Requirement R2 clarifies that protections must be afforded to INSM data collected in support of Requirement R1 and must continue to be afforded to INSM data retained in requirement R3.	
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	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF supports the proposed language for CIP-015-1 Requirement R2 and Measurement M2.	

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 agrees with the comments submitted by EEI.	
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 and NAGF comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your support. Please see responses to EEI's and NAGF's comments.	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
The wording of requirement R2 and M2 clearly outline the requirements. MRO NSRF suggests a non-substantive change to re-order Requirements (and consequently Measures) R2 and R3 so that this requirement refers back to requirements already read vs. both back and forward to a requirement not yet read, making the standard easier to understand when reading it in order. If adopted the reference to R3 would need to be changed to R2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this question in alignment with the EEI.	
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 responding to this question in alignment with the EEI.	
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	
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.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
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.	
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.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
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.	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Tyler Schwendiman - ReliabilityFirst - 10	
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.	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
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.	
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.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
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.	
Richard Jackson - U.S. Bureau of Reclamation - 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.	
Ben Hammer - Western Area Power Administration - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 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.	
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.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
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.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	

4. Based on industry feedback, Requirement R3 and Measure M3 were revised for clarity of data retention requirements and a note following Requirement R3 was added to ensure that there is an explicit statement about not requiring the retention of data that is not relevant to anomaly network activity detected. Do you agree with the language proposed in Requirement R3 and Measure M3? If you do not agree, please provide your recommendation, and if appropriate, technical, or procedural justification.

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments: "We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to NPCC RSC’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 disagrees with the proposed language in Requirement R3. For example, CIP-007 R4, states that logs are retained for 90 days. The current draft of CIP-015 does not state a time frame to keep logs. How long should REs keep evidence? Should each RE make this determination and possibly write up a policy on saving data for a time frame of their choosing? If that is the case, each RE will be able to keep a different amount of data, some more some less. Would that be acceptable to an auditor or is that the intent of the drafting team? SRP prefers language added in the requirement stating how each RE must store x days of data at minimum or that each RE must retain data to show compliance.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.	
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	
Within the cyber security industry, the average time required to detect an intrusion is 200+ days. Thus, the volume of data required to sufficiently analyze when and/or how the anomalous activity began will create a cost-prohibitive data storage issue. If it is the intent of CIP-015-1 to be focused solely on the specific activities occurring at the time of discovery of an anomalous activity, this is no longer an issue; however, ACES does not believe that is the intent of the SDT or the FERC order. Furthermore, the language for retention included in R3 does not reference a reportable incident, nor an attempt to compromise, and is not tied to CIP-008. ACES believes Requirement R1 should have inputs into and be closely tied to the reportable requirements within CIP-008.	
Likes 0	
Dislikes 0	

Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.	
Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
R3: SPP asks that the SDT provide additional clarity around what is a reasonable duration for data retention. The current language places the burden on the entity to determine that duration, but records retention for ERO compliance monitoring and enforcement could significantly lengthen how long an entity is required to retain the data and place a significant cost on an entity for storing that data. A more prescriptive time period (e.g., 90 days, 180 days) would seem reasonable to include in the R3 requirement language, and precedence currently exists in the NERC CIP Standards for security event logging today (CIP-007-6, R4, Part 4.3).	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	

Dominion Energy is concerned about the use of the word "detailed" when describing the level of INSM data that should be retained. What information would be required to be retained that is not relevant to the anomalous activity if full packet capture data is not required?	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT updated the Note in Requirement R2 (previous Requirement R3). Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture date, 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 comments. Please see responses to IRC SRC's comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	No
Document Name	
Comment	

We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	No
Document Name	
Comment	
We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.	
Ruchi Shah - AES - AES Corporation - 5	

Answer	No
Document Name	
Comment	

AES supports MRO NSRF comments listed below

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 comments. Please see responses to MRO NSRF's comments.	
Ben Hammer - Western Area Power Administration - 1,6	
Answer	No
Document Name	
Comment	
See response to question 1	
Likes 0	
Dislikes 0	
Response	
Thank you for your comment. Please see response to Question 2.	

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 language "internal network security monitoring data (full packet capture data, etc.) that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2" is not sufficiently clear and will lead to auditing challenges. The concept of "relevant to anomalous network activity" can be construed in many ways, and different auditors may come to different conclusions regarding the relevance of certain network activity. To ensure consistency with R1.2 and R1.3, the SRC recommends that the determination of what is "*anomalous"* be left to those sub-requirements and the term *"relevant to"* be replaced with the term "related to". The SRC recommends the following note language revision: Note: The Responsible Entity is not required to retain detailed internal network security monitoring data (full packet capture data, etc.) that is not related to network activity detected and evaluated under Requirement R1, Parts 1.2 and 1.3. It is also unclear what action the phrase "until the action is complete" is intended to refer to, and the SRC recommends that this be clarified.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT updated the Note in Requirement R2 (previous Requirement R3). Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture date, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	No
Document Name	
Comment	

We are concerned about demonstrating compliance of a record retention in support of R1 due to retention timelines that expire once event investigation activities are completed. There is an analogy with CIP-07 Requirement 4 that requires a 90-day retention for security log event investigations.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.	
Ijad Dewan - Ijad Dewan On Behalf of: Emma Halilovic, Hydro One Networks, Inc., 1; - Ijad Dewan	
Answer	No
Document Name	
Comment	
We would prefer to have a defined timeframe for data retention similar to CIP-007 Requirement R4.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.	
Roger Perkins - Southern Maryland Electric Cooperative - 1	
Answer	No
Document Name	

Comment	
SMECO agrees with ACES comments: Within the cyber security industry, the average time required to detect an intrusion is 200+ days. Thus, the volume of data required to sufficiently analyze when and/or how the anomalous activity began will create a cost-prohibitive data storage issue. If it is the intent of CIP-015-1 to be focused solely on the specific activities occurring at the time of discovery of an anomalous activity, this is no longer an issue; however, ACES does not believe that is the intent of the SDT or the FERC order.Furthermore, the language for retention included in R3 does not reference a reportable incident, nor an attempt to compromise, and is not tied to CIP-008. ACES believes Requirement R1 should have inputs into and be closely tied to the reportable requirements within CIP-008.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to ACES's comments.	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA appreciates the clarification in R3 and the Technical Rationale regarding which data must be retained. However, we note that there is potential for voluminous data to be flagged as "anomalous", especially during the time it will take to tune the process. BPA does not support the retention timeframe "until the action is complete." It is unclear if this phrase is referring to the evaluation required by Part 1.3, the determination of further actions required by Part 1.3, or the "further actions" mentioned in Part 1.3. BPA notes that the latter could include risk mitigation or recovery actions that span a considerable length of time.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. If further action is determined to be necessary in accordance with Requirement R1, Part 1.3, the data shall be retained until that further action is completed.	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding to this question in alignment with the EEI.	
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 is responding to this questions in alignment with the EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments.	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	

Answer	Yes
Document Name	
Comment	
Southern Indiana Gas & Electric Co. d/b/a CenterPoint Energy Indiana South (SIGE) agrees that Requirement R3 and Measure M3 were revised for clarity of data retention requirements. SIGE also appreciates the note at the end of the requirement, as it helps add clarity.	
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	
CenterPoint Energy Houston Electric, LLC (CEHE) agrees that Requirement R3 and Measure M3 were revised for clarity of data retention requirements. CEHE also appreciates the note at the end of the requirement, as it helps add clarity.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes

Document Name	
Comment	
Ameren agrees with and supports EEI and NAGF comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's and NAGF's comments.	
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 comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	

The NAGF supports the proposed language for CIP-015-1 Requirement R3 and Measurement M3.	
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	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.	

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 revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.	
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.	
Likes 0	
Dislikes 0	

Response	
Thank you for your support. Please see responses to EEI’s comments.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	Yes
Document Name	
Comment	
We support EEI's comments: EEI agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. 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; Foung 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	
The wording of the Note under Requirement R3 can be improved by revising it to state “(for example, full packet capture data, etc.)”, or alternately “(e.g. full packet capture data, etc.)”. As the Note is currently written, an entity may assume that “full packet capture” is a	

requirement for internal network security monitoring in Requirement R1, whereas the intent of the Note seems to be to provide an example of the data that is not required to be obtained. This change would be non-substantive and could be made in the final ballot.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. The DT updated the Note in Requirement R2 (previous Requirement R3). Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture date, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE agrees with EEI comment: EEI agrees with revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI's comments.	
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 revisions to Requirement R3 and Measurement M3 and appreciates the inclusion of the note in Requirement R3 that clarifies that the expectation is to retain internal network security data that is relevant to anomalous network activity detected in Requirement R1, Part 1.2, addressing concerns associated with the volume of data requiring retention from the previous draft.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Please see responses to EEI’s comments.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Only retaining the data that is associated with network activity determined to be anomalous could lead to a forensics issue if the traffic is within the current baseline and not pre-identified as an anomaly. With the current language of the standard this data would not be retained. Responsible Entities should reevaluate the “normal” traffic baseline on a periodic basis to ensure that they are identifying any anomalous activity to address this risk.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	

Answer	Yes
Document Name	
Comment	
No additional comment.	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	Yes
Document Name	
Comment	
Manitoba Hydro does not believe the note is necessary but does not object to adding the note if it promotes consensus. Manitoba Hydro suggests that the word “detailed” and parenthetical example be removed to clarify and preserve the intent of the note. [Note: The Responsible Entity is not required to retain internal network security monitoring data that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.]	
Likes 0	
Dislikes 0	
Response	

Thank you for your support. The DT updated the Note in Requirement R2 (previous Requirement R3). Note: The Responsible Entity is not required to retain ~~detailed~~ internal network security monitoring data ~~(full packet capture date, etc.)~~ that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Who gets to or how is it determined what data is not relevant? What if an entity doesn't think it was relevant but an auditor does?	
Likes 0	
Dislikes 0	
Response	
Thank you for your support. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged.	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 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	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Marcus Bortman - APS - Arizona Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Richard Jackson - U.S. Bureau of Reclamation - 1	
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.	

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.	
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.	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
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.	

Karen Artola - CPS Energy - 1,3,5 - Texas RE	
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.	
Erik Gustafson - PNM Resources - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Thank you for your support.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
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.	

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.	
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.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE understands the phrase “until the action is complete” to mean that if further action is determined to be necessary in accordance with Requirement Part 1.3, the data shall be retained until that further action is completed. Texas RE agrees with retaining network activity determined to be anomalous until the action is completed, except for anomalous activity that was determined to be part of a Cyber Security Incident that was part of an attempt to compromise as defined by the entity’s CIP-008 process or was part of a Reportable Cyber Security Incident. For anomalous network activity that was determined to be part of a Cyber Security Incident that was part of an attempt to compromise as defined by the entity’s CIP-008 process or was part of a Reportable Cyber Security Incident Texas RE recommends setting the retention period to one calendar year after the completion of the action.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged. Anything under CIP-008 process would follow that process and would not be part of the INSM process. Entities should consider CIP-008 when designing their data retention process for proposed Reliability Standard CIP-015-1.

5. 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	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy supports EEI Comments which state: EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.	

Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to EEI's comments.	
Rebika Yitna - Rebika Yitna On Behalf of: David Weekley, MEAG Power, 3, 1; Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	
Document Name	
Comment	

The Technical Rationale document can use additional editing to align with the edited standards. For example. On Page 6 near the bottom there is a section titled “Data Collection Locations” that in the first sentence redlines out “collection locations” in favor of “feed(s)” which aligns with the standard. Yet the section title continues to focus on “Locations” as well as the content within the section, even though the standard is now related to “feed(s)”.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Technical Rationale has been updated to align with the edited proposed Reliability Standard CIP-015-1.	
Tyler Schwendiman - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
The Drafting Team should consider requirement language pertaining to the testing of their program put in place to detect anomalous activity on the Responsible Entity’s network to ensure their controls are working properly. The Drafting Team should also consider requirement language pertaining to the ability to detect instances where the protections put in place are not working properly to reduce the response time of the program not functioning as intended similar to CIP-007-6 R4 P4.2.2.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Each entity will need to do what makes sense for their environment. The DT recognizes 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 and FAQ that can be leveraged. This is an appropriate internal control that the Responsible Entity could implement.	

Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	
Document Name	
Comment	
Displaying the requirement, parts and subparts in the table format with the "Applicable Systems, Requirements, and Measures," is the preferred formatting.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT received positive feedback in not utilizing the table format in proposed Reliability Standard CIP-015-1.	
Denise Sanchez - Denise Sanchez On Behalf of: Diana Torres, Imperial Irrigation District, 1, 6, 5, 3; George Kirschner, Imperial Irrigation District, 1, 6, 5, 3; Jesus Sammy Alcaraz, Imperial Irrigation District, 1, 6, 5, 3; Tino Zaragoza, Imperial Irrigation District, 1, 6, 5, 3; - Denise Sanchez	
Answer	
Document Name	
Comment	
We operate within a geographical region characterized by limited access of local academic enrichment opportunities for young professionals in cybersecurity. Moreover, this project will require significant technical effort, substantial capital investment, and the augmentation of staffing resources.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. 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. 893[3] 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.

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

Answer	
Document Name	

Comment

Black Hills Corporation agrees with EEI comments:

EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide.

Likes 0	
Dislikes 0	

Response

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

Richard Vendetti - NextEra Energy - 5

Answer	
Document Name	
Comment	
NEE agrees with EEI comment: EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing" from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide. Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to EEI's comments.	
Mike Magruder - Avista - Avista Corporation - 1	
Answer	
Document Name	
Comment	

We support EEI's comments: EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide. Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 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	
Document Name	
Comment	
ITC supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	

Thank you for your comments. Please see responses to EEI’s comments.	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI suggests removing the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale because CMEP Practice Guides are intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities, not in the context in which the Technical Rationale is intended for use by registered entities. The current Technical Rationale provides sufficient justification and clarifies the intent of the Drafting Team when developing the CIP-015 Standard without including a reference to the Practice Guide. Further, the Practice Guide was developed prior to the drafting of this Standard, and it would be more appropriate to consider the development of ERO endorsed Implementation Guidance where registered entities seek examples or approaches on ways to comply with a Standard or requirement within a Standard. EEI sees opportunity for the development of Implementation Guidance documents on topics such as the development and implementation of a risk-based rationale for implementing data collection feeds, and controls to protect INSM data.	

Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The Technical Rationale has been updated to read: ~~The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing[2]”~~ The Responsible Entity’s existing process(es) should be referenced to determine if the INSM system and its components are 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	
Answer	
Document Name	
Comment	
Duke Energy supports EEI comments.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 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 has no additional comments.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

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:

> 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."

> 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 comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system. The risk-based rationale should be used to describe why an entity chose not to monitor specific ESP networks if they choose not to monitor the entirety of their ESP networks. Examples are provided in the Technical Rationale and FAQ to describe how those risk-based decisions could be made. The DT believes that including "risk-based rationale" is more encompassing than alternative language proposed by several commenters. 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.	
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 the comments of the Edison Electric Institute (EEI) for Question #5.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to EEI's comments.	
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 comments. 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	
Document Name	
Comment	
Southern Company agrees with the additional comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Chantal Mazza On Behalf of: Nicolas Turcotte, Hydro-Quebec (HQ), 1, 5; - Chantal Mazza	
Answer	
Document Name	
Comment	
The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements.	

Likes 0

Dislikes 0

Response

Thank you for your comments. 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.

Ben Hammer - Western Area Power Administration - 1,6

Answer

Document Name

Comment

The standards drafting committee needs develop NERC defined terms and definitions for the following terms:

- Anomalous Network activity
- Network Data Feeds

The standards drafting committed needs to address wither the INSM systems constitutes an EACM(S) and or BCSI repository or both.

The drafting team needs to provide a reasonable compliance solution, acceptance of work of others, or changes to the requirements in CIP-004, CIP-005, CIP-007, and CIP-010 to assist Responsible Entities (REs) with the ability to maintain compliance for cloud-based solutions for INSM.

Likes 0

Dislikes 0

Response

Thank you for your comments. The DT considered whether or not to create a NERC Glossary term for “anomalous.” The Merriam-Webster dictionary defined anomalous as:

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.

The INSM system may be classified as BCSI or EACMS per the existing processes for each entity.

Changes to requirements and compliance solutions of CIP-004, CIP-005, CIP-007, and CIP-010 is outside of the scope of Project 2023-03.

David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Michael Russell - Massachusetts Municipal Wholesale Electric Company - 5 - NPCC	
Answer	
Document Name	
Comment	

The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 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 DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	
Document Name	
Comment	
The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. 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 DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.	

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	

CEHE would like to restate that 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.

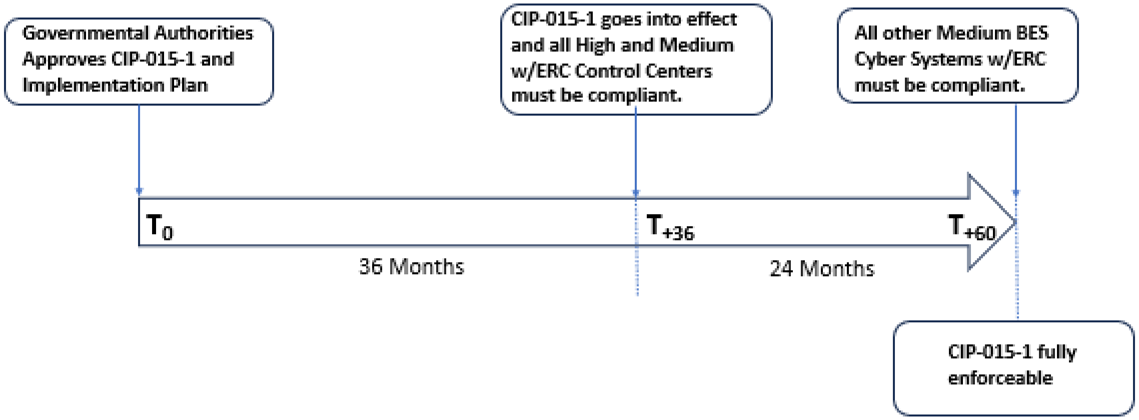
CEHE also supports the comments submitted by the Edison Electric Institute as it relates to the removal of the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale.

Likes 0	
Dislikes 0	

Response

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

The DT provided an implementation timeframe of 36 months for high impact and medium impact control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the 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.


Governmental Authorities Approves CIP-015-1 and Implementation Plan
CIP-015-1 goes into effect and all High and Medium w/ERC Control Centers must be compliant.
All other Medium BES Cyber Systems w/ERC must be compliant.
T0
T+36
T+60
36 Months
24 Months
CIP-015-1 fully enforceable

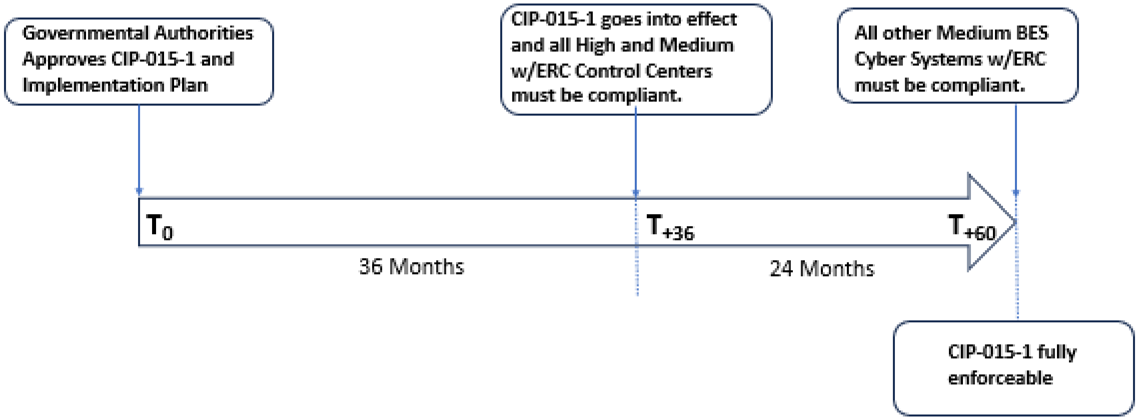
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	
Document Name	
Comment	
SIGE would like to restate that SIGE does not agree with the implementation plan because implementation in substation facilities will be extremely time consuming. Implementation within a high impact 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. 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. SIGE also supports the comments submitted by the Edison Electric Institute as it relates to the removal of the reference to the ERO Enterprise Compliance Monitoring and Enforcement (CMEP) Practice Guide “Network Monitoring Sensors, Centralized Collectors, and Information Sharing” from the Technical Rationale.	
Likes 0	

Dislikes 0	

Response

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

The DT provided an implementation timeframe of 36 months for high impact and medium impact control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the 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.


Governmental Authorities Approves CIP-015-1 and Implementation Plan
CIP-015-1 goes into effect and all High and Medium w/ERC Control Centers must be compliant.
All other Medium BES Cyber Systems w/ERC must be compliant.
T_0
T_{+36}
T_{+60}
36 Months
24 Months
CIP-015-1 fully enforceable

Daniel Gacek - Exelon - 1

Answer	
Document Name	

Comment

Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc. so that the utilities can have a standardize method to determine **in-scope high and medium impact BCS with ERC**

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system.

Mia Wilson - Mia Wilson On Behalf of: Joshua Phillips, Southwest Power Pool, Inc. (RTO), 2; - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	
Document Name	

Comment

Implementation Plan: Entities will require sufficient time to research and identify new technology solutions to meet the new INSM requirements. Implementation could require significant changes and/or additions to existing network architectures. Therefore, SPP appreciates and endorses the 36-month timeframe for implementation.

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	
Document Name	

Comment

ACES believes the proposed requirements of CIP-015-1 are out of order and should be re-numbered. As currently written, Requirement R2 references Requirements R1 and R3; therefore, ACES believes it should be placed after the current Requirements R1 and R3.

ACES would like to thank the SDT for its hard work.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT discussed your comment and reversed Requirements R2 and R3 to better align with the order of the requirements.

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

SRP recommends having baseline defined in the Measures rather than in the technical guidance.

Likes 0	
Dislikes 0	

Response

Thank you for your comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system.	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	
Exelon is requesting the Standard Drafting Team to clarify and provide additional guidance on what are the risk factors we need to consider to calculate risk-based score and whether those risk factors should be standardized across industry or not. Either within the Measures, Technical Rationale, etc. so that the utilities can have a standardized method to determine **in-scope high and medium impact BCS with ERC**.	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. The DT recognizes 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 and FAQ that can be leveraged to access the risk of not monitoring specific networks in an entity's environment when they develop an INSM system.	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments:	

"The SDT would benefit for taking more time between ballot postings. Switching the order of appearance in R2 and R3 may flow more logically in expressing the relation between requirements."	
Likes 0	
Dislikes 0	
Response	
Thank you for your comments. Please see responses to NPCC RSC’s comments.	