Comment Report

Project Name:	2023-03 Internal Network Security Monitoring | Draft 1
Comment Period Start Date:	12/14/2023
Comment Period End Date:	1/17/2024
Associated Ballots:	2023-03 Internal Network Security Monitoring (INSM) CIP-007-X IN 1 ST 2023-03 Internal Network Security Monitoring (INSM) CIP-007-X Non-Binding Poll IN 1 NB 2023-03 Internal Network Security Monitoring (INSM) Implementation Plan IN 1 OT

There were 75 sets of responses, including comments from approximately 198 different people from approximately 116 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC and explicitly excluded low impact BCS and medium impact BCS without ERC. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are excluded for INSM data collection? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

2. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC. Do you agree that the cyber assets included within the standard will further reliability within the CIP-networked environment? If you disagree, what high impact BCS and medium impact Cyber Assets with ERC should be included within or excluded from the standard in order to address reliability within the CIP-networked environment? Please explain why and if any identified BCS should or should not be included.

3. Order No. 887 also references “CIP-Network Environment” that could include Cyber Assets, such as PCA, EACMS, and PACS that are associated with high-impact BCS and medium-impact BCS with ERC. The SDT used a risk-based approach to provide guidance as to which network communications between these Cyber Assets. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are included or excluded for INSM data collection consistent with Order No. 887? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

4. The Project 2023-03 SDT did not intend for every CIP network interface to be monitored with INSM. Each responsible entity should perform an assessment of their applicable CIP network communications and determine what is most critical to monitor. Do you agree that the current language in Draft 1 of proposed CIP-007-X, Requirement R6, Part 6.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

5. The Project 2023-03 SDT held extensive conversations about the term “baseline” and what alternatives there might be to avoid confusion with the term baseline used in Reliability Standard CIP-010-4, Requirement R1, Part 1.1. Ultimately, the SDT could not find a suitable alternative and believed that it should be clear that a network communications baseline would be entirely different from a software baseline used in Reliability Standard CIP-010-4. Do you agree that the SDT’s use of the term “network communications ‘baseline’” is clear in Requirement R6 Part 6.3? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

6. The Project 2023-03 SDT held extensive discussions regarding the use of the term “anomalous.” The SDT did not intend for responsible entities to use only signature-based tools to detect suspicious activity, and thus, the use of “anomalous” was descriptive of approaches that looked at a normal network communications baseline and identified deviations. The intent was to not only discover known malicious communications, but to identify unusual communications that need to be investigated, and the SDT decided that the term “anomalous” was the appropriate term to use to describe that methodology. Do you agree that that the term “anomalous” effectively describes those methodologies? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

7. The Project 2023-03 SDT tried to clarify that the process to determine appropriate action regarding anomalous activity in Requirement R6, Part 6.4 occurred prior to escalation and potential initiation of a responsible entity’s CIP-008 process. Do you agree that the SDT was clear that this occurs before the determination of a Cyber Security Incident? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

8. Throughout proposed Requirement R6, the Project 2023-03 SDT tried to create a requirement that was objective based and allow latitude for various INSM methodologies and technologies to be used now and in the future. Do you agree that the SDT was successful in this endeavor? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

9. Do you agree with the Implementation Plan for Draft 1 of proposed CIP-007-X of 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

10. Do you agree that the modifications made in Draft 1 or proposed CIP-007-X are cost effective? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Preformance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Coporation (SPC)	1	MRO
					Angela Wheat	Southwestern Power Administration	1	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO

					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
Anne Kronshage	Anne Kronshage			Public Utility District No. 1 of Chelan County - Voting Group	Anne Kronshage	Public Utility District No. 1 of Chelan County	6	WECC
					Diane Landry	Public Utility District No. 1 of Chelan County	1	WECC
					Rebecca Zahler	Public Utility District No. 1 of Chelan County	5	WECC
					Joyce Gundry	Public Utility District No. 1 of Chelan County	3	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
WEC Energy Group, Inc.	Christine Kane	3		WEC Energy Group	Christine Kane	WEC Energy Group	3	RF
					Matthew Beilfuss	WEC Energy Group, Inc.	4	RF
					Clarice Zellmer	WEC Energy Group, Inc.	5	RF
					David Boeshaar	WEC Energy Group, Inc.	6	RF
Southern Company -	Colby Galloway	1,3,5,6	MRO,RF,SERC,Texas RE,WECC	Southern Company	Matt Carden	Southern Company -	1	SERC

Southern Company Services, Inc.						Southern Company Services, Inc.		
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Leslie Burke	Southern Company - Southern Company Generation	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
Eversource Energy	Joshua London	1		Eversource	Joshua London	Eversource Energy	1	NPCC
					Vicki O'Leary	Eversource Energy	3	NPCC
FirstEnergy - FirstEnergy Corporation	Mark Garza	4		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF

Michael Johnson	Michael Johnson		WECC	PG&E All Segments	Marco Rios	Pacific Gas and Electric Company	1	WECC
					Sandra Ellis	Pacific Gas and Electric Company	3	WECC
					Frank Lee	Pacific Gas and Electric Company	5	WECC
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	2	SERC
Black Hills Corporation	Rachel Schuldt	6		Proj 2023-03 INSM	Rachel Schuldt	Black Hills Corporation	6	WECC
					Micah Runner	Black Hills Corporation	1	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Josh Combs	Black Hills Corporation	3	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
					Alain Mukama	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC

					Jeffrey Streifling	NB Power Corporation	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
					John Pearson	ISO New England, Inc.	2	NPCC
					Harishkumar Subramani Vijay Kumar	Independent Electricity System Operator	2	NPCC
					Randy MacDonald	New Brunswick Power Corporation	2	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					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
					Glen Smith	Entergy Services	4	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
					ALAN ADAMSON	New York State Reliability Council	10	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	1	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	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC

Coordinating Council					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC
Lower Colorado River Authority	Teresa Krabe	5		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Tim Kelley	Tim Kelley		WECC	SMUD and BANC	Nicole Looney	Sacramento Municipal Utility District	3	WECC
					Charles Norton	Sacramento Municipal Utility District	6	WECC
					Wei Shao	Sacramento Municipal Utility District	1	WECC
					Foung Mua	Sacramento Municipal Utility District	4	WECC
					Nicole Goi	Sacramento Municipal Utility District	5	WECC
					Kevin Smith	Balancing Authority of Northern California	1	WECC
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Gary Dollins	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Olivia Olson	Sho-Me Power Electric Cooperative	1	SERC

					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
					Heath Henry	NW Electric Power Cooperative, Inc.	3	SERC
					Tony Gott	KAMO Electric Cooperative	3	SERC
					Micah Breedlove	KAMO Electric Cooperative	1	SERC
					Brett Douglas	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Mark Riley	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Chuck Booth	Associated Electric Cooperative, Inc.	5	SERC
					Jarrod Murdaugh	Sho-Me Power Electric Cooperative	3	SERC
Santee Cooper	Vicky Budreau	3		Santee Cooper	Rene Free	Santee Cooper	1,3,5,6	SERC
					Christie Pope	Santee Cooper	1,3,5,6	SERC
					Chris Mcneil	Santee Cooper	1,3,5,6	SERC
					Troy Lee	Santee Cooper	1,3,5,6	SERC

					Wanda Williams	Santee Cooper	1,3,5,6	SERC
					Jordan Steele	Santee Cooper	1,3,5,6	SERC
					Bridget Coffman	Santee Cooper	1,3,5,6	SERC
					Shedrick Snider	Santee Cooper	1,3,5,6	SERC
					Kevin Gainey	Santee Cooper	1,3,5,6	SERC
					Lachelle Brooks	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC

1. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC and explicitly excluded low impact BCS and medium impact BCS without ERC. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are excluded for INSM data collection? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

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

Answer	No
Document Name	

Comment

1. The use of undefined terms (e.g., EACMS that performs access control) creates ambiguity in interpretation and identification of applicable systems & associated communications.

2. The standard should be focused on BES Cyber Systems and PCAs (e.g., those systems inside the ESP). Inclusion of non-BES Cyber Assets, coupled with the ambiguity of non-glossary defined criterion is overly broad and diminishes the focus on protecting the most important systems.

Likes 0	
Dislikes 0	

Response

Karen Artola - CPS Energy - 1,3,5 - Texas RE

Answer	No
Document Name	

Comment

With the increased concern of critical infrastructure infiltration by foreign adversaries, excluding low impact BCS presents a moderate level of risk and vulnerability.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

OPG supports NPCC Regional Standards Committee’s comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Reclamation recommends that the Applicable Systems language be changed to reduce confusion if an EACMS or PACS should be protected.

From:

High Impact BES Cyber Systems and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

To:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and

- PCA	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
Southern Indiana Gas & Electric Co. d/b/a CenterPoint Energy Indiana South (SIGE) believes the proposed language does not explicitly exclude low impact BCS and medium impact BCS without ERC, it does not mention low impact. It explicitly includes applicable systems, but it does not explicitly exclude anything.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	

PG&E agrees with the current language in Draft 1.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees it is clear that low impact BCS and medium impact BCS without ERC are not included in the proposed requirement.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	

Comment	
NEE supports EEI comments: “EEI agrees that the proposed changes to CIP-007 explicitly exclude low impact BCS and medium impact BCS without ERC. “	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes

Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the proposed changes to CIP-007 explicitly exclude low impact BCS and medium impact BCS without ERC.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Exelon agrees that the proposed changes to CIP-007 explicitly exclude low impact BCS and medium impact BCS without ERC.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Yes. Applicable systems clearly exclude medium impact BCS without ERC and low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	

Yes. Applicable systems clearly exclude medium impact BCS without ERC and low impact BCS.	
Likes 0	
Dislikes 0	
Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments by EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	Yes
Document Name	EEI Near Final Draft Comments _ Project 2023-03 INSM Draft 1 Rev 0d 1_16_2024.docx
Comment	

See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

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	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Jennifer Neville - Western Area Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
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	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Order No. 887 explicitly included high impact BCS and medium impact BCS with ERC. Do you agree that the cyber assets included within the standard will further reliability within the CIP-networked environment? If you disagree, what high impact BCS and medium impact Cyber Assets with ERC should be included within or excluded from the standard in order to address reliability within the CIP-networked environment? Please explain why and if any identified BCS should or should not be included.

Megan Melham - Decatur Energy Center LLC - 5

Answer	No
Document Name	

Comment

We appreciate the effort of the SDT in trying to interpret FERC Order No. 887 and revise the CIP standards to address it appropriately. We agree that the draft language includes the high impact BCS and medium impact BCS with ERC. However, the “CIP-networked environment” diagram supplied in the Technical Rationale is ambiguous. Suggest revise scoping to exclude traffic between EACMS and PACS and include traffic between EACMS Intermediate System and EACMS EAP. Intermediate Systems and EAPs are primary paths to cyber assets within the ESP. PACS communication systems may be configured in such a way that it is completely separate from the OT environment. By including communication between EACMS and PACS, the standard could unintentionally be increasing the scope of many CIP compliance programs.

Likes 0	
Dislikes 0	

Response

Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company agrees that Order 887 explicitly included high impact BCS and medium impact BCS with ERC. However, the question concerns the 'cyber assets included in the standard' which is a larger scope. Given the unclear scoping of 6.1 as currently written, requirement part 6.1 itself, the diagrams showing some ‘out of scope’ PACS components, and statements in the TR that state that not all Cyber Assets involved will be of sufficient monitoring value to include, Southern Company concludes that not every Cyber Asset in the ‘CIP Networked Environment’ should be included in mandatory scope.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No
Document Name	
Comment	
The term CIP-networked environment is too broad and leaving it undefined presents compliance challenges. In FERC Order 887, EACMS and PACS are neither excluded nor included. LCRA believes that FERC's intention was to include INSM in the trusted zone of the ESP only. This would include only BCAs and PCAs, which is commensurate with the risk.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
It is unclear why EACMS that perform only monitoring function are excluded from the requirements. An EACMS that only monitors, such as SIEM, could be compromised should there be any deletion or modification of logs concealing the malicious activities or traffic. Thus, it should also be included in order to improve the reliability.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
The term CIP-networked environment is too broad and leaving it undefined presents compliance challenges. In FERC Order 887, EACMS and PACS are neither excluded nor included. LCRA believes that FERC's intention was to include INSM in the trusted zone of the ESP only. This would include only BCAs and PCAs, which is commensurate with the risk.	
Likes 0	
Dislikes 0	

Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
While PNMR agrees with the cyber assets included within the standard, it does not necessarily believe that this requirement as a whole increases reliability but more so, security.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
The question is somewhat unclear. Interpreted as if there is a subset of “scoping” besides the High Impact and Medium Impact with ERC. When reviewing the Technical Rationale, there are subsets of EACMS etc. The “scoping” mechanism is unclear when reviewing the proposed CIP-007 R6.1. It is also unclear what “will further reliability within the CIP-networked environment”. How would this be measured? Is this purely subjective? A Responsible Entity could disagree. EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well. While I agree that including these cyber assets will improve reliability through increased cyber security, however we noticed that only EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.	
Likes 0	
Dislikes 0	
Response	
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

The question is somewhat unclear. Interpreted as if there is a subset of “scoping” besides the High Impact and Medium Impact with ERC. When reviewing the Technical Rationale, there are subsets of EACMS etc. The “scoping” mechanism is unclear when reviewing the proposed CIP-007 R6.1.

It is also unclear what “will further reliability within the CIP-networked environment”. How would this be measured? Is this purely subjective? A Responsible Entity could disagree.

EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.

While I agree that including these cyber assets will improve reliability through increased cyber security, however we noticed that only EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Duke Energy notes that the defined term BCS is inclusive of devices classified as BCA and not other associated classified cyber assets, and therefore agrees with the BCS that were selected for inclusion. However, Duke Energy does not agree that the additional cyber assets included in the proposed standard’s applicability further reliability within the CIP-networked environment. We do not support the interpretation that the CIP-networked environment is inclusive of EACMS and PACS-classified cyber assets that do not reside within an ESP. Since V5 took effect, the only constructs for trust zones defined within the CIP standards are the ESP applicable for High/Medium BCS and the Low Electronic Access Controls required by CIP-003 Attachment 1 Section 3. There is no trust zone that the standards contemplate for EACMS and PACS devices that reside outside the above identified zones. Therefore, the intention to monitor east-west traffic within a trust zone in FERC Order 887 most clearly fits with the expectation that INSM is applied within applicable ESPs to increase network visibility beyond the existing perimeter-based controls required by CIP-005. Moving beyond the BCS and outside the ESP takes the focus off the most critical environments for monitoring. INSM systems are likely to generate extreme volumes of data as entities mature their implementations. Large data volumes will require significant investment of time and resources to generate meaningful baselines of network traffic, especially for large entities with diverse software solutions across their various BCS and EACMS. An unclear and overly large scope for the initial INSM implementation threatens to create alarm/alert fatigue that will hamper the ability of entities to detect and respond to threats to their most critical systems residing within their ESPs.

Likes 0	

Dislikes 0	
Response	
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	
FERC Order 887 did not include EACMS and PACS. There is no requirement that EACMS or PACS be protected by a firewall, so to include them as part of "inside the CIP-networked environment" is a huge stretch for the Standards Drafting Team to make and scope creep of Order 887. Including EACMS and PACS in the requirement for INSM, where monitoring is only required between them, does not further the reliability and security inside the CIP networked environment. There is likely to be a lot of "noise" that must be tuned out when trying to monitor only traffic between certain EACMS and PACS devices since they can be inside more open networked environments. The security value of monitoring only the "INSM" (east-west) traffic assumes that you must first be compromised by non-INSM (north-south) traffic before you would potentially see anomalous INSM communication; this makes very little security sense.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well. While I agree that including these cyber assets will improve reliability through increased cyber security, however we noticed that only EACMS that perform access control functions are in scope for High and Medium Impact Cyber Systems. Is it intentional that EACMS that perform monitoring functions are excluded? The risks of deletion or modification of logged data by an adversary on the EACMS performing monitoring such as a SIEM could conceal their presence, and these devices should therefore be in scope as well.	
Likes 0	

Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The “CIP-networked environment” diagram supplied in the Technical Rationale is ambiguous. Suggest revise scoping to exclude traffic between EACMS and PACS, and include traffic between EACMS Intermediate System and EACMS EAP. Intermediate Systems and EAPs are primary paths to cyber assets within the ESP.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	

Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is of the opinion that the proposed changes will improve the security of the CIP-networked environment.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	

Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI is of the opinion that the proposed changes will improve the security of the CIP-networked environment.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees that the draft language includes the high impact BCS and medium impact BCS with ERC. However, the question refers to CIP-networked environment, which has created confusion about the SDT’s goal for responses. To refer to a CIP-networked environment high impact BCS and medium impact Cyber Assets with ERC does not align with current CIP-005 language in R1.1 which requires medium and high impact BCS and their associated Protected Cyber Assets “connected to a network via a routable protocol shall reside within a defined ESP.” Inclusion of EACMS and PACs in the standard draft language goes beyond Order No. 887.	
Likes 0	

Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: “ EEI is of the opinion that the proposed changes will improve the security of the CIP-networked environment. “	
Likes 0	

Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees that the cyber assets included within the standard will further reliability within the “CIP-network environment”**.**	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	

AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes R6.2 could conceivably lower security posture if the transport and/or repository of such logging information is compromised.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
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	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
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 believes that whether any other ballot pool member agrees with the directives in Order 887 is moot. Questions about what types of BCS should or should not be addressed by revisions to one or more CIP Standards should have been raised after FERC issued its Notice of Proposed Rulemaking about INSM on January 27, 2022.	
Likes 0	
Dislikes 0	
Response	

3. Order No. 887 also references “CIP-Network Environment” that could include Cyber Assets, such as PCA, EACMS, and PACS that are associated with high-impact BCS and medium-impact BCS with ERC. The SDT used a risk-based approach to provide guidance as to which network communications between these Cyber Assets. Do you agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are included or excluded for INSM data collection consistent with Order No. 887? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No
Document Name	

Comment

The scoping of PCA is clear. However, the language “that perform access control functions” is not clear. The language would be improved by specifying what type of “access control functions” are applicable (e.g., for authentication). Consider the following revisions for the High and Medium Impact scoping language in the Applicable Systems section:

1. EACMS that perform authentication functions;

2. PACS that rely upon EACMS that perform authentication functions; …

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The use of undefined terms (e.g., EACMS that performs access control) creates ambiguity in interpretation and identification of applicable systems & associated communications.

As the standard in current state does not direct that PACS be protected by an EACMS, entities are dis-incentivized to protect PACS due to the additional regulatory exposure created by the draft language.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	
Comment	
While sufficient, there is always the possibility that there could be confusion or disagreement over which EACMS provide “access control” only. The SDT may wish to consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS)” Furthermore, it is our understanding from discussions that only authenticating EACMS need to be included. If this is not the intent additional clarifying language (under Applicable Systems) is needed.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the SDT INSM seminar, it isn’t clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. I don’t feel the term CIP-Network Environment should be used here when it can’t be found in the standard requirements. The diagram in the presentation is required for clarity on what the applicable systems are, but a presentation isn’t where entities should be getting that information. Excluding EACMS devices that perform monitoring functions is not advisable in my opinion. Also stating that 100% coverage is not required leads to potential confusion. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be	

subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

BPA supports Chelan PUD’s remarks proposing modification of the draft scoping language in the Table R6 – INSM - Applicable Systems section to reduce confusion about which EACMS and PACS are in scope:

1. EACMS that perform authentication functions;

2. PACS that rely upon EACMS that perform authentication functions; …”

For clarity, BPA also recommends the drafting team reinstate the definitions pertaining to “Applicable Systems” on page 6 to include definitions for any new terms used in the next draft, especially the phrase “PACS that rely upon…”

Likes 0	
Dislikes 0	

Response

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	No
Document Name	

Comment

The Standard Drafting Team has done a very good job at identifying additional components in the “CIP-Network Environment” that need to be monitored without increasing the scope further than necessary. The technical rational describes the scope, including a diagram. The language used in the applicability section EACMS “that performs access control functions” does not match the diagram and intent of the Standard Drafting Team. This phrase would include all access control EACMS, including the following that were marked as out of scope on the diagram:

An EACMS that contains an EAP, for example a firewall

An EACMS that acts as an Intermediate System, for example a jump host

To clarify the EACMS in scope it is suggested to use the wording “EACMS that perform authentication for more than one CIP Cyber Asset”. This better matches the diagram presented, where traffic going to a firewall (an access control EACMS) is out of scope, however traffic to a two factor authentication server or active directory server would be in scope.

Manitoba Hydro suggests removing PACS from the applicability section, as there are no other network security requirements that apply to PACS. Traffic from EACMS that support PACS would already be included if the EACMS was in scope.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

AECI supports comments provided by the MRO group.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

PG&E does not agree the language clearly indicates what is in-scope and out of scope. The FERC Order was for “internal” communications, but the current language does not clearly indicate this and could be interpreted by auditors to include traffic outside of the ESP, such as those to PACS and EACMS outside of the ESP. PG&E recommends to clearly indicate that communications outside of the ESP to devices such as PACS and EACMS are not in scope.

Likes 0	

Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE is concerned with scoping EACMS to only those that perform access control in Requirement R6. Certain monitoring systems, such as a SIEM, may be an attack priority and should be included in internal network monitoring. SIEMs contain logs for all CIP networked devices configured to send applicable security logs to them. An attack against the SIEM could subsequently result in an attacker removing logs of their activity in order to prolong time to discovery and hinder recovery efforts. Texas RE recommends removing the language "that perform access control functions" from the Applicable Systems column. Texas RE noticed the SDT identified “PACS that rely upon EACMS that perform access control functions” as an Applicable System in Requirement R6. Texas RE requests clarity on what this is intended to be mean. Texas RE noticed the technical rationale document states “CIP-networked environment is inclusive of communications between a PACS and EACMS. Communications between a PACS and any other device is out of scope.” (Page 6). The technical rationale should not create or modify requirement language. If these types of communications are intended to be out of scope, this should be represented in enforceable requirement language, either by explicitly defining what communications are in scope or by explicitly defining what communications are out of scope.	
Likes 0	
Dislikes 0	
Response	
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	
The order does not specifically reference EACMS and PACS, therefore it is not part of the CIP-network environment.	
Likes 0	
Dislikes 0	

Response

Byron Booker - Oncor Electric Delivery - 1

Answer	No
Document Name	

Comment

Oncor stands in agreement on the comments made by EEI that states:

"EEI remains concerned that the applicability section for Requirement R6 is not sufficiently clear and needs additional work in order to fully clarify the specific applicability of PCAs, EACMs and PACSs in Draft 1 of CIP-007-X. While we have suggested some edits to the applicability section in our response to question 4, further work may still be needed beyond replacing “access control” with “authentication control”. Nevertheless, we do feel authentication control is superior to access control, as proposed."

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Tri-State agrees with MRO provided comments:

"While sufficient, there is always the possibility that there could be confusion or disagreement over which EACMS provide “access control” only. The SDT may wish to consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS).

Furthermore, it is our understanding from discussions that only authenticating EACMS need to be included. If this is not the intent additional clarifying language (under Applicable Systems) is needed."

Likes 0	
Dislikes 0	

Response

Jeffrey Icke - Colorado Springs Utilities - 5

Answer	No

Document Name	
Comment	
FERC Order 887 references a CIP-Network Environment in the context of assets within an Electronic Security Perimeter. The Order does not mention PCA, EACMS, or PACS. The standard language including those devices is a significant expansion of the scope of the FERC Order. While PCA are, by definition, within the Electronic Security Perimeter, EACMS and PACS are not necessarily located within the ESP and should not be included in the standard.	
Likes 0	
Dislikes 0	
Response	
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	
As documented in FERC Order 887, "INSM is a subset of network security monitoring that is applied within a “trust zone,” such as an electronic security perimeter. For the purpose of this rulemaking, the trust zone applicable to INSM is the CIP-networked environment," the trusted zone protected by a firewall. Including EACMS and PACS, which are not required to be protected by an ESP, Electronic Access Point (EAP), or required to be in a “trust zone” does not align with intent of the SAR or the FERC Order, which is to perform network monitoring of traffic between devices ***within*** a trusted zone. The intent of the SAR was to close the gap that currently exists in CIP-005, which is the inability to detect lateral movement of a compromised system. The way the requirements are currently scoped, EACMS and PACS are included when they are not even required to be in a trusted zone, and only traffic between them proposed for monitoring. Therefore, this becomes a detective control to determine if a device has already been compromised. EACMS and PACS should be removed from the project scope and the INSM requirements should be moved to CIP-005. Including EACMS and PACS in the scope, significantly increases the cost and complexity of the INSM requirement as many PACS are spread throughout different geographical locations and networks, significantly increasing the cost and complexity of implementing the requirements, with little security benefit to gain since any attack would likely come from a Cyber Asset that is not classified as an EACMS or PACS. SMUD recommends removing EACMS and PACS from the project scope and moving the INSM requirements to CIP-005 as a network and BCS level control rather than leaving it in CIP-007 where Cyber Asset level controls are typically required.	
Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
Duke Energy's understanding of the CIP-Networked Environment and its use in the order was that it meant to capture High BCS and Medium BCS without ERC, while using language that could align in the future with the requirement for Lows for which there is no ESP. With that disclaimer, we believe that the applicability clauses " EACMS that perform access control functions" and "PACS that rely upon EACMS that perform access control functions" is meant to convey a subset of EACMS and PACs, and it is unclear exactly which subset of these assets is intended to be included. This applicability will necessitate entities performing subclassifications of their EACMS and PACS to determine potential scope. We recommend the Applicable Systems be scoped to High Impact BES Cyber Systems and their associated PCA and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA. If the SDT is unable to align to this approach that leverages the existing CIP-required trust zones, we would request that the SDT invest the necessary time to define terms to clearly articulate which subsets of EACMS and PACS are relevant for this standard.	
Likes 0	
Dislikes 0	
Response	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Without discouraging implementation of ISNM, the administrative burden of classifying the NERC-defined term of EACMS more granularly diminishes the value the SDT intended. The reliability gained by requiring INSM on this subset of systems does not outweigh the increased cost or additional documentation needed to prove compliance.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	

MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE supports EEI comments: “ The applicability section for Requirement R6 is not sufficiently clear and needs additional work to fully clarify the specific applicability of PCAs, EACMs and PACSs in Draft 1 of CIP-007-X. While we have suggested edits to the applicability section in our response to question 4, further work may still be needed beyond what has been provided. The proposed changes, as provided in our response to question 4 below, provide greater clarity while aligning with the intent of this project. “	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	

Comment

NST believes Order 887 is clearly intended to apply exclusively to high or medium impact BCS inside ESPs, its use of the phrase, "CIP-networked environments" notwithstanding. There is no mention in the Order of "CIP" devices that may be outside ESPs, such as EACMS and PACS, and we believe this was in fact intentional. We note, further, there are numerous statements in the Order that reinforce this opinion, including:

"INSM is a subset of network security monitoring that is applied within a 'trust zone,' such as an electronic security perimeter." (Paragraph 2)

"We find that, while the CIP Reliability Standards require monitoring of the electronic security perimeter and associated systems for high and medium impact BES Cyber Systems, the CIP-networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack." (Paragraph 3)

"Finally, INSM provides insight into east- west network traffic happening inside the network perimeter, which enables a more comprehensive picture of the extent of an attack compared to data gathered from the network perimeter alone." (Paragraph 13)

"The NOPR explained that including INSM requirements in the CIP Reliability Standards would ensure that responsible entities maintain visibility over communications between networked devices within a trust zone rather than simply monitoring communications at the network perimeter access point(s) (***i.e., at the boundary of an electronic security perimeter as required by the current CIP requirements***)." (emphasis added) (Paragraph 14)

"While the CIP Reliability Standards require monitoring of inbound and outbound internet communications at the electronic security perimeter, the currently effective CIP Reliability Standards do not require INSM *within* trusted CIP-networked environments for BES Cyber Systems." (Paragraph 20)

In addition, the Q2 2023 issue of the highly respected and widely consulted ReliabilityFirst newsletter, "The Lighthouse," is titled, "Preparing for Internal Network Security Monitoring (INSM)." It opens with the following statements: "Internal Network Security Monitoring, or INSM, is the practice of understanding what is going on inside your networks. For the purposes of the CIP Standards, that means understanding what network traffic is occurring ***within*** your Electronic Security Perimeters (ESPs)." (emphasis added). With all due respect to the SDT's "risk-based approach" (not described in the Technical Rationale document) to deciding certain types of CIP devices outside of ESPs should** be in scope, NST believes the drafting team has far exceeded the authorization granted by the Standards Committee's approval, on August 23, 2023, of the INSM Standard Authorization Request.

** NST notes that on Page 5 of the Technical Rationale document, the SDT states, "The term CIP-networked environment used in the context of standards development in support of project 2023-03 (Internal Network Security Monitoring) ***shall*** be inclusive of the following (adjusted for clarity for the purposes of showing SDT development of revisions to CIP-007-X):" (emphasis added). We assume the use of the word, "shall" was unintentional.

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	

Comment

Reclamation recommends that the Applicable Systems language be changed to reduce confusion if an EACMS or PACS should be protected.

From:

High Impact BES Cyber Systems and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

To:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Likes 0	
Dislikes 0	

Response

Jennifer Neville - Western Area Power Administration - 6

Answer	No
Document Name	

Comment

Need to clarify which EACMS provide “access control” only. Consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS)”. Also please clarify that only authenticating EACMS need to be included or update the language under Applicable Systems to explain.

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3

Answer	No
Document Name	

Comment

Entergy has concerns regarding the Applicable Systems of the proposed standard and the use of new terms and/or scope increase, in particular with “PACS that rely upon EACMS that perform access control functions”. It is not clear on what “rely” means in this context. Additionally, this would expand scope beyond network security requirements for PACS, or incentivize entities to reduce security for compliance margin. For example, under the existing CIP-005 standard PACS are not required to reside in an ESP or have their External Routable Connectivity flow through an Electronic Access Point on an EACMS. Under this standard an entity could utilize a non-CIP interface on a EACMS with a segmented network to provide perimeter protections/access control as a best security practice, but this would be outside CIP-005 scope. With the proposed standard as drafted because that EACMS is providing security controls to the PACS, even though not required by CIP-005, the PACS would be brought into scope of this standard. This could incentivize entities to move PACS away from EACMS systems providing access control to less secure pathways totally outside CIP scope to avoid an increase in compliance requirements.

Likes 0	
Dislikes 0	

Response

David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

A better investment for such a huge shift for some companies would be to create secure DMZ zones that must include some type of IPS inspection for malicious code and ensure all traffic to EACMS and PACS go through a firewall and IPS.

Several new non-NERC Glossary terms were created. The CIP-Network Environment and network communications are not defined – should have a sample definition for review.

Clarity around access control function should occur. Either this should be a defined term or the use of this should be clarified with examples. Using NIST, a definition might be:

Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space. Sources: NIST SP 800-192 under Access Control. NISTIR 7316 under Access Control.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The NAGF does not agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that the devices (e.g. PCA, EACMS, and PACS) are included or excluded for INSM data collection consistent with Order No. 887. Question 3 indicates “The SDT used a risk-based approach to provide guidance as to which network communications between these Cyber Assets” which appears to be missing a part of the statement. How did the SDT team risk-based approach exclude EACMs and PACs that are only performing monitoring functions? As described in the technical guidance, “Threat actors commonly take steps to hide their actions, and very often need to work for an extended period within targeted environments to develop disruption capabilities.” In either case, the NAGF would refer the SDT back to Order 887 in that the network traffic in scope for INSM is communications within an ESP between other Cyber Assets within that “trust zone” also referred to as east west traffic. The inclusion of EACMS and PACS goes beyond the scope of INSM and the current Draft 1 creates confusion as to the intent of the requirements commingling “Network Security Monitoring” principles which include devices outside of the ESP or “trust zones”.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Tacoma Power does not agree with the addition of EACMS and PACS to this Standards Project. While Order 887 specifically calls out the “CIP-Networked Environment”, there is no mention of EACMS or PACS in the Order. In reviewing previous FERC Orders that have applied to EACMS and PACS, these system types are specifically identified within the Order, see FERC Order No. 850 as an example.

Likes 0	
Dislikes 0	

Response

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

Is this question asking to “scope” the PCA, EACMS, and PACS based on a risk based approach (Impact Rating); outside of what is listed in the applicable systems (What PCA, EACMS, and PACS? Are communicating and to where?)

Please clarify if the evaluation approach is CIP-007 R6.1 “…Collection methods should provide security value to address the perceived risks.”

Recommend a potential more granular definition for EACMS regarding access control. This is unclear of the impact between regional Responsible Entity interpretations / applications, and auditing.

The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the SDT INSM seminar, it isn’t clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. I don’t feel the term CIP-Network Environment should be used here when it can’t be found in the standard requirements. The diagram in the presentation is required for clarity on what the applicable systems are, but a presentation isn’t where entities should be getting that information.

Excluding EACMS devices that perform monitoring functions is not advisable in my opinion. Also stating that 100% coverage is not required leads to potential confusion. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.

Likes 0	
Dislikes 0	

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer	No
Document Name	

Comment

“See comments submitted by the Edison Electric Institute”

Likes 0	
Dislikes 0	

Response

Whitney Wallace - Calpine Corporation - 5

Answer	No
Document Name	

Comment

A better investment for such a huge shift for some companies would be to create secure DMZ zones that must include some type of IPS inspection for malicious code and ensure all traffic to EACMS and PACS go through a firewall and IPS.

Several new non-NERC Glossary terms were created. The CIP-Network Environment and network communications are not defined – should have a sample definition for review.

Clarity around access control function should occur. Either this should be a defined term or the use of this should be clarified with examples. Using NIST, a definition might be:

Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space. Sources: NIST SP 800-192 under Access Control. NISTIR 7316 under Access Control.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer	No
Document Name	

Comment

Is this question asking to “scope” the PCA, EACMS, and PACS based on a risk based approach (Impact Rating); outside of what is listed in the applicable systems (What PCA, EACMS, and PACS? Are communicating and to where?)

Please clarify if the evaluation approach is CIP-007 R6.1 “…Collection methods should provide security value to address the perceived risks.”

Recommend a potential more granular definition for EACMS regarding access control. This is unclear of the impact between regional Responsible Entity interpretations / applications, and auditing.

The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the SDT INSM seminar, it isn't clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. I don't feel the term CIP-Network Environment should be used here when it can't be found in the standard requirements. The diagram in the presentation is required for clarity on what the applicable systems are, but a presentation isn't where entities should be getting that information.

Excluding EACMS devices that perform monitoring functions is not advisable in my opinion. Also stating that 100% coverage is not required leads to potential confusion. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

We believe the standard is clear for assets within the ESP, however there is room for confusion when assets are located outside the ESP. Specifically, if the PACS is outside the "CIP-Network Environment" then it should be out of scope as well.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The definition for EACMS currently reads, "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems." PNMR understands the STD's intent to focus on EACMS designed for access control, but specifically designating types of EACMS (and PACS) for the Applicable Systems seems to indirectly change definitions. This change also deviates from all existing "Applicable Systems" in current Standards.

Additionally, to more closely align with language related to other "Applicable Systems" in other requirements, PNMR believes the "Applicable Systems" should read, "EACMS with access control functions."

Finally, PNMR is unclear on the exact meaning behind, “PACS that rely upon EACMS that perform access control functions.”	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
The applicability section for Requirement R6 is not sufficiently clear and needs additional work to fully clarify the specific applicability of PCAs, EACMs and PACSs in Draft 1 of CIP-007-X. While we have suggested edits to the applicability section in our response to question 4, further work may still be needed beyond what has been provided. The proposed changes, as provided in our response to question 4 below, provide greater clarity while aligning with the intent of this project.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support comments as provided by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	

Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	

We believe the standard is clear for assets within the ESP, however there is room for confusion when assets are located outside the ESP. Specifically, if the PACS is outside the “CIP-Network Environment” then it should be out of scope as well.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
Please see LCRA’s response to question 2 above. The term “CIP-networked environment“ is ambiguous and not defined in FERC Order 887 to include PACS and EACMS.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	

The EACMS that perform only monitoring function should also been included. Although described in technical rationale, it is better to properly add "CIP-Network Environment" in NERC's glossary of terms.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
The FERC order specifically addressed High and Medium-Impact assets. Extending the proposed standard to associated EACMS and PACS exceeds the scope of the FERC order and they should be removed. GSOC believes that the order as written could include communication between High or Medium assets and their corresponding PACS/EACMS. Nevertheless, there is a lack of clarity regarding the inclusion of ALL EACMS and PACS communications within the Applicable Systems. If the intent is to capture such communications, this can be feasibly achieved through tools already monitoring the High and Medium assets from within their ESP.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Please see LCRA’s response to question 2 above. The term “CIP-network environment“ is ambiguous and not defined in FERC Order 887 to include PACS and EACMS.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	

Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Consider defining “CIP Networked Environment” in the glossary of terms or the standard itself. Additionally, “CIP Networked Environment “could be further defined to make it clearer on what is included and excluded.	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) does not agree that the current language in Draft 1 of proposed CIP-007-X clearly indicates that these devices are included or excluded for INSM data collection consistent with Order No. 887. CEHE believes that the use of “EACMS that perform access controls” and “EACMS” from the “Interpretation of the CIP-Network Environment” diagram presented in the SDT webinar is unclear. “EACMS” seems to refer to authentication mechanisms, but EACMS in some environments, if not most, refer to firewalls that do not perform authentication, but do perform access control. CEHE suggests using the phrase “EACMS that perform authentication functions” as it relates to the “CIP-Network Environment.”	
Likes 0	
Dislikes 0	

Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company agrees with the comments by EEI. Additionally, Southern Company would like to state a concern for the record that the scope of the current draft does not clearly align with what is stated in the Order and the SAR. The only reference to EACMS and PACS in the Order is in section 21 and is in relation to the existing requirement CIP-007 R4.1.3. While it is clear in the Order that the scope of CIP-networked environment extends beyond the Electronic Security Perimeter, it would be helpful to industry in the future if all applicable Cyber Assets intended to be included were clearly stated in the Order and the SAR.	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE believes that “PACS that rely upon EACMS that perform access control functions” is not entirely clear. It is not clear what “rely upon EACMS that perform access control functions” means. It could be interpreted to mean the PACS relies on the EACMS to validate that an individual is allowed to have physical access to a NERC CIP area, or it could be interpreted to mean the PACS relies on the EACMS to validate a username and password in order to log into the PACS server/system. SIGE would like to see further clarification included.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	

While sufficient, there is always the possibility that there could be confusion or disagreement over which EACMS provide “access control” only. The SDT may wish to consider using the phrase “EACMS that perform access control functions (excluding monitoring-only EACMS)”

Furthermore, it is our understanding from discussions that only authenticating EACMS need to be included. If this is not the intent additional clarifying language (under Applicable Systems) is needed.

Likes 0	
Dislikes 0	

Response

Megan Melham - Decatur Energy Center LLC - 5

Answer	No
Document Name	

Comment

The CIP-Network Environment needs to be added to the glossary of terms. Without a clear definition and the diagram in the Technical Rationale, it isn’t clear when EACMS and PACS should be included. The entities and the audit teams need to have better clarity. This leaves the possibility of a disconnect between the entities and auditors. We don’t recommend using the term CIP-Network Environment when it can’t be found in the glossary of terms. The diagram in the Technical Rationale is required for clarity on what the applicable systems are, but is still ambiguous enough that it leaves too much interpretation between systems that an entity identifies as applicable versus what an auditor would identify as applicable systems.

Stating that 100% coverage is not required without providing a minimum threshold or other guidance on an acceptable level of coverage leads to potential confusion. Different entities define and evaluate acceptable levels of risk differently. If the RE determines that 50% coverage is sufficient, but an auditor feels that 80% was the intent of the standard, then we could be subject to PNC. The language in a standard must leave little room for interpretation, because the RE will tend to interpret on the lower side for cost and effort savings, while an auditor is then free to interpret on the high side and issue PNCs.

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 3

Answer	No
Document Name	

Comment

Exelon is responding in support of the comments provided by EEI.

Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Prior CIP SARs have scoped a projects applicable system(s) by what is stated in the Project Scope section of a SAR. To rely on the undefined term “CIP-Network Environment” to further scope this project creates confusion for industry. The project scope of the SAR only listed – The Standard Drafting Team (SDT) will create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order. The scope of the project will include: &bull; All high impact BES Cyber Systems, and &bull; All medium impact BES Cyber Systems with ERC The scope of the project should not extend to: &bull; medium Impact BES Cyber Systems without ERC or &bull; low impact BES cyber systems	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	

Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC). In addition, MISO asks the SDT to consider adding the term "CIP-networked environment" to the NERC Glossary. As this term is used in FERC Order 887, defining it could be useful in identifying which EACMS (e.g. those used for authentication only and traversing the EAP) are applicable.	
Likes 0	
Dislikes 0	
Response	

4. The Project 2023-03 SDT did not intend for every CIP network interface to be monitored with INSM. Each responsible entity should perform an assessment of their applicable CIP network communications and determine what is most critical to monitor. Do you agree that the current language in Draft 1 of proposed CIP-007-X, Requirement R6, Part 6.1 is clear to that intent? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
To avoid numerous interpretations of if '100 percent coverage is not required' then what is required. Consider the following - 'Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets, as determined by the Responsible Entity, to monitor and detect anomalous activity. Collection methods should ensure visibility to identify known or suspected malicious communications.'	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	

We agree that it is clear the way Requirement R6.1 is written that not every CIP network interface is required to be monitored with INSM. However, without providing a guidance document on what provides “security value” and is considered “critical” there is enough ambiguity that there can be disagreements between what an entity has identified within its own processes and procedures and what an auditor considers to be “critical” and provides “security value”, leading to the auditor issuing PNCs. How can an auditor or entity determine they did enough?

If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.

Please clarify what a CIP network interface is. Is this supposed to be data collection points? The minimum coverage should be defined to avoid any confusion.

Likes 0	
Dislikes 0	

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

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

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

The language in this question is indicative of the drafting team’s intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility (“100 percent coverage is not required”) leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity” in place of the 100% statement as more consistent with the expressed intent.

Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

While in one respect it seems clear as to the intent, it is not clear how an entity is supposed to make this determination and be able to defend its decision during an audit. An auditor may easily determine that an entity has not gone far enough regarding what is being collected. The language in R6.1 clearly states that INSM should provide security value and does not require 100% coverage. This leaves the risk assessment leading to INSM implementation scope up to the Responsible Entity. However, the scope described in the CIP-007-X Technical Rationale includes the scope in broad prescriptive terms. The Technical Rationale should clearly state that the Technical Rationale does not determine the scope, but only potential limits of the scope, subject to the risks identified and prioritized by the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company agrees with the comments by EEI. In addition, Southern Company offers the following comments:

Requirement R6.1 currently has an abundance of phrases that entities must prove with evidence. For example, it can be read that the entity must describe how *each* collection location or method can monitor and detect anomalous activity and specifically all connections, devices, and network communications.

Southern Company suggests 6.1 be rewritten so that it does not force entities to “prove the negative” of the gap between what they did monitor and the 100% of all applicable Cyber Assets. The following wording is recommended to align with this concept:

“One or more process(es) to identify network data collection locations the Responsible Entity determines provide sufficient security value in determining anomalous activity.” With this wording concept, the evidence burden shifts to providing a reasonable monitoring location identification process and then evidence it was followed.	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
While in one respect it seems clear as to the intent, it is not clear how an entity is supposed to make this determination and be able to defend its decision during an audit. An auditor may easily determine that an entity has not gone far enough regarding what is being collected. The language in R6.1 clearly states that INSM should provide security value and does not require 100% coverage. This leaves the risk assessment leading to INSM implementation scope up to the Responsible Entity. However, the scope described in the CIP-007-X Technical Rationale includes the scope in broad prescriptive terms. The Technical Rationale should clearly state that the Technical Rationale does not determine the scope, but only potential limits of the scope, subject to the risks identified and prioritized by the Responsible Entity.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
CIP-007-X, Requirement R6, Part 6.1 indicates 100% is not required. This statement leaves a lot open for interpretation by an auditor. If an entity is collecting 50% of the data is it compliant or will an auditor determine this is not enough. Without a firm number communicated to auditors and entities it would be difficult to ensure Part 6.1 is interpreted the same way.	
Likes 0	
Dislikes 0	
Response	

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
It is challenging to be compliant without prescription and the lack of clarity could cause contention with regulators that disagree with a Registered Entity’s interpretation and risk analysis. While the requirement states that 100 percent coverage is not required, we believe the language is still too vague to sufficiently inform LCRA’s determination of the level of coverage necessary for compliance with the requirement.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
Part 6.1 includes "network communications." However, the term introduces ambiguity as it is unclear which specific network communications require identification, such as protocols, ports, applications, or other elements. The mandate for 100% coverage is not explicitly stated, creating uncertainty about the extent of coverage required. There is a lack of clarity in defining the parameters or criteria determining the necessary coverage.	

The statement, "Collection methods should provide security value to address the perceived risks," prompts questions about the nature of the perceived risks. It raises considerations about whether it necessitates the formal execution of a risk assessment specifically targeting internal networks. Additionally, there is uncertainty about the expectation to document identified risks and articulate how an entity's data location and methods effectively mitigate these risks, extending beyond the implementation of INSM (Industrial Network Security Monitoring). The measures proposed in the Standard imply that the sole requirement is the provision of architecture documents or similar documentation. If this interpretation is accurate, the language within the updated Requirement could be simplified to explicitly state, "Identify network data collection locations and methods designed to offer visibility of network communications (excluding serial) among relevant Cyber Assets." This modification would enhance precision and eliminate potential misinterpretations.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
It is not clear to the intent. “what is more critical to monitor” and “security value to address the perceived risks” is vague; additional details/specifics should be provided.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
It is challenging to be compliant without prescription and the lack of clarity could cause contention with regulators that disagree with a Registered Entity’s interpretation and risk analysis. While the requirement states that 100 percent coverage is not required, we believe the language is still too vague to sufficiently inform LCRA’s determination of the level of coverage necessary for compliance with the requirement.	
Likes 0	
Dislikes 0	
Response	

Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	No
Document Name	
Comment	
AZPS does not believe the current language is clear in regard to performing an assessment of applicable CIP network communication and determination of what is most critical to monitor. AZPS recommends “Perform an assessment to identify locations and methods to collect network communication data (excluding serial) between applicable Cyber Assets, including connections, devices, and routable protocol network communications, to monitor and detect deviations from a normal network communications baseline. Identified locations and methods are not required to provide 100% coverage, but rather should be determined based on risk, criticality and security value.”	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Avista agrees with EEI that it does not fully support the currently proposed language for both the Applicability Section and Requirements. Relative to the Applicability Section, “access control” is insufficiently narrow and should be replaced with authentication control to more clearly define the desired scope. Additionally, the statement “100 percent coverage is not required” is too ambiguous and may create unintentional compliance expectations for	

registered entities. This statement should be deleted, and the last sentence should be expanded to include the statement “as determined by the responsible entity.” See the proposed changes in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1.   EACMS that perform **authentication** control functions;

{C}2.   PACS that rely upon EACMS that perform **authentication** control functions; and

{C}3.   PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1.   EACMS that perform **authentication** control functions;

{C}2.   PACS that rely upon EACMS that perform **authentication** control functions; and

{C}3.   PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect

anomalous activity, including connections, devices, and network **communications (excluding communications between ESPs).** Collection methods should provide security value to address the perceived risks**, as determined by the responsible entity**.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1

Answer	No
Document Name	

Comment

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

Likes 0	
Dislikes 0	

Response

Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the comments as provided by EEI and NSRF.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI does not fully support the proposed language in Requirement R6, Part 6.1. Our concerns include the applicability section (affecting all of Requirement R6 parts), noting that PACS need not be specifically included in the applicability section. Noting that if the goal is to capture the authentication related traffic, then there is no need to monitor PACS to collect that traffic (i.e., it should be sufficient to simply monitor at the switch the EACMS). Next, we are not supportive of the statement that “100 percent coverage is not required”. The language is too ambiguous and may create unintentional compliance expectations for registered entities. EEI is also concerned that identifying network communications may not be sufficient because there are types of “networks” where there is no monitoring technology available. To address this concern, we suggest adding “routable protocol” prior to network communications throughout R6. To address these concerns, we offer the following edits in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

1. EACMS devices that authenticate for other CIP Cyber Assets; **and**
2. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS devices that authenticate for other CIP Cyber Assets; **and**
2. PCA.

Requirements

Identify network data collection locations and methods that provide **security value and** visibility of network communications (excluding serial) to monitor and detect anomalous activity, including connections, devices, and **routable protocol** network communications.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The intent does not seem to be reflected in what is written. The sentence, “100 percent coverage is not required” opens too many avenues for vastly different interpretations across industry. If the intent is for an entity to design how it will collect network data in a balanced manner with criticality in mind, then it should be stated. The “100 %” sentence could be replaced with, “Determine which CIP network communications are most critical to monitor. The monitoring and collection methods should provide security value to address the perceived risks.”

Perhaps a different approach could be to clarify that the objective is not to monitor the endpoints. The language could state that 100% of monitoring endpoints in not required.

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	No
Document Name	

Comment

Comments: Avista agrees with EEI that it does not fully support the currently proposed language for both the Applicability Section and Requirements. Relative to the Applicability Section, “access control” is insufficiently narrow and should be replaced with authentication control to more clearly define the desired scope. Additionally, the statement “100 percent coverage is not required” is too ambiguous and may create unintentional compliance expectations for registered entities. This statement should be deleted, and the last sentence should be expanded to include the statement “as determined by the responsible entity.” See the proposed changes in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1. EACMS that perform **access authentication** control functions;

{C}2. PACS that rely upon EACMS that perform **access authentication** control functions; and

{C}3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1. EACMS that perform **access authentication** control functions;

{C}2. PACS that rely upon EACMS that perform **access authentication** control functions; and

{C}3. PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network **communications (excluding communications between ESPs)**. **100 percent coverage is not required.** Collection methods should provide security value to address the perceived risks**, as determined by the responsible entity**.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
Please clarify what a CIP network interface is. Is this (EAP, EACMS, PACS etc) or a “bump in the wire” tool? The intent of CIP-007 R6.1 is unclear; and perhaps overloaded on what R6.1 is trying to do. It is clear that 100% coverage isn’t required, but what provides “security value” and is considered “critical” isn’t. A guidance document is required. How can an auditor or entity determine they did enough? There should be a guidance document to help both the entities and auditors feel confident they are compliant with the new requirements. If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	No
Document Name	
Comment	
The language of the controls should state that a risk-based strategy or systematic approach should be in place to evaluate network communications to identify the most critical communications to monitor.	
Likes 0	
Dislikes 0	
Response	

Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
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	
Please clarify what a CIP network interface is. Is this (EAP, EACMS, PACS etc) or a “bump in the wire” tool? The intent of CIP-007 R6.1 is unclear; and perhaps overloaded on what R6.1 is trying to do. It is clear that 100% coverage isn’t required, but what provides “security value” and is considered “critical” isn’t. A guidance document is required. How can an auditor or entity determine they did enough? There should be a guidance document to help both the entities and auditors feel confident they are compliant with the new requirements. If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	

While the current wording mentions that "100% coverage is not required", that leaves the possibility for an auditor to demand an arbitrary amount that is less than 100%. The SRC recommends adding verbiage indicating that the collection locations and methods should be commensurate to the risk posed as determined by the Responsible Entity.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Tacoma Power does not agree that the intent is clearly expressed in the language of Requirement 6 Part 6.1. The term "perceived risk" is not a well-defined or measurable quantify and as such, would be difficult to implement. There is no definition within the Requirement language that clarifies what "internal" means in the internal network security monitoring term. Tacoma Power suggests defining internal network security monitoring.

Tacoma Power suggests the following for the language of Requirement 6 Part 6.1:

"Identify network data collection locations and methods that provide visibility of network communications (excluding serial) within the network subnets of applicable CIP Systems, to monitor and detect anomalous activity, including connections, devices, and network communications between applicable CIP Systems.

Note: While complete coverage is not required, the implemented collection methods should increase the probability of detecting an attack that has bypassed network perimeter-based security controls."

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The NAGF recommends that the SDT change Requirement 6.1 to state, "Identify network data collection location(s) and methods required to internally monitor applicable CIP networked environments that provide security value to address organizational risks."

Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The language of the controls should state that a risk-based strategy or systematic approach should be in place to evaluate network communications to identify the most critical communications to monitor.	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP is concerned with the anticipated scope of Part 6.1 and believes the language should allow more flexibility for Responsible Entities to determine the network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity. SPP proposes the following language for Part 6.1: Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous network activity indicative of an attack in progress.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
The standard as drafted provides the latitude for entities to “identify network data collection locations and methods” as the first sentence of the question states. However, there is no identification in the standard of the expectations of entities to “perform an assessment” and “determine what is critical to monitor” as the second question of the sentence implies. If this is the expectation to assess and define, and entities will be audited against that assessment and definition, then it should be clearly detailed as an expectation in the standard.	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
The language in this question is indicative of the drafting team’s intent to provide needed flexibility to Responsible Entities in designing their INSM system. However the phrase (“100 percent coverage is not required”) leaves how much less than 100% is sufficient to the second-guessing of any auditor. Suggest continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity” in place of the 100% statement as more consistent with the expressed intent.	
Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	

Comment

Reclamation recommends that the Applicable Systems language be changed to reduce confusion if an EACMS or PACS should be protected.

From:

High Impact BES Cyber Systems and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS that perform access control functions;
- PACS that rely upon EACMS that perform access control functions; and
- PCA.

To:

High Impact BES Cyber Systems and their associated:

- EACMS;
- PACS; and
- PCA

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

- EACMS;
- PACS; and
- PCA

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NST believes the statement in the “Requirements” column of proposed Part 6.1, "100 percent coverage is not required," would almost certainly be both difficult to understand and difficult to audit. We note that the SDT addressed these concerns during the January 3, 2024 INSM webinar and provided a good explanation of what "percent coverage" was intended to mean (paraphrasing, a Responsible Entity's most important obligation is to design a collection system capable of detecting potentially malicious traffic on network segments between in-scope Cyber Assets, and so long as this is accomplished, it should be possible to justify not monitoring outbound and inbound traffic on every port on every device, which in some instances could be technically infeasible and/or prohibitively expensive). NST suggests either (a) deleting the "100 percent" statement, along with the one that follows ("Collection methods should provide security value to address the perceived risks.") or (b) moving them to the "Measures" Section of 6.1 if the SDT feels it is an important thing for Responsible Entities to understand.

Likes 0	
Dislikes 0	

Response

Richard Vendetti - NextEra Energy - 5

Answer	No
Document Name	

Comment

“ EEI does not fully support the proposed language in Requirement R6, Part 6.1. Our concerns include the applicability section (affecting all of Requirement R6 parts), noting that PACS need not be specifically included in the applicability section. Noting that if the goal is to capture the authentication related traffic, then there is no need to monitor PACS to collect that traffic (i.e., it should be sufficient to simply monitor at the switch the EACMS). Next, we are not supportive of the statement that “100 percent coverage is not required”. The language is too ambiguous and may create unintentional compliance expectations for registered entities. EEI is also concerned that identifying network communications may not be sufficient because there are types of “networks” where there is no monitoring technology available. To address this concern, we suggest adding “routable protocol” prior to network communications throughout R6. To address these concerns, we offer the following edits in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1.   EACMS devices that **perform access control functions** authenticate for other CIP Cyber Assets; **and**

{C}**2.   PACS that rely upon EACMS that perform access control functions; and**

{C}3.   PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1.   EACMS devices that authenticate for other CIP Cyber Assets; **and**

{C}**2. PACS that rely upon EACMS that perform access control functions; and**

{C}3. PCA.

Requirements

Identify network data collection locations and methods that provide **security value and** visibility of network communications (excluding serial) **between applicable Cyber Assets** to monitor and detect anomalous activity, including connections, devices, and **routable protocol** network communications. **100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.** “

Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	

Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	
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 proposes the following two options to improve Requirement R6 Part 6.1**:** “Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications, **as determined by the Responsible Entity**. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.” Or “**As determined by the Responsible Entity,** identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.”	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	No
Document Name	
Comment	

The statement "100 percent coverage is not required." does not provide sufficient clarity on what, or how much must be collected. The next statement, "Collection methods should provide security value to address the perceived risks.", appears to try and qualify this, but still does not provide a sufficient guidepost for measuring compliance. Additionally, 'coverage' is not defined and further adds to the ambiguity.	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
Although NIPSCO agrees with the SDT's intent, "100 percent coverage is not required," seems ambiguous. This statement does not seem necessary in the language of the Standard as the Applicable Systems table defines the scope. This should be added to the Technical Rationale.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No
Document Name	
Comment	
The language in Part 6.1 is a rogue auditor's dream. If 100 percent is not required, then what percentage is acceptable and who gets to decide? If collection methods "should provide security value to address the perceived risks", then who gets to define "security value" or "perceived risks"?	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	No
Document Name	

Comment

Tri-State agrees with MRO provided comments:

"The language in this question is indicative of the drafting team's intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility ("100 percent coverage is not required") leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity" in place of the 100% statement as more consistent with the expressed intent.

Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome."

Likes 0	
Dislikes 0	

Response

Byron Booker - Oncor Electric Delivery - 1

Answer	No
Document Name	

Comment

Oncor stands in agreement on the comments presented by EEI that states:

"EEI does not fully support the proposed language in Requirement R6, Part 6.1. Among our concerns is the statement that "100 percent coverage is not required". While we appreciate the intent of this language, we feel it is too ambiguous and may create unintentional compliance expectations for registered entities. EEI is also concerned that simply identifying network communications may not be sufficient because there are types of "networks" where there is no monitoring technology available. To address this concern, we suggest adding "routable protocol" prior to network communications throughout R6. To address EEI's concerns, we offer the following edits in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

{C}1. EACMS **with that perform access authentication** control **for other CIP systems functions**;

{C}2. PACS that rely upon EACMS **with that perform access authentication** control **for other CIP systems functions**; and

{C}3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

{C}1. EACMS **with that perform access authentication** control **for other CIP systems functions**;

{C}2. PACS that rely upon EACMS **with that perform access authentication** control **for other CIP systems functions**; and

{C}3. PCA.

Requirements

Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and **routable protocol** network **communications**. **100 percent coverage is not required.** Collection locations and methods should provide security value to address the perceived risks**, as determined by the responsible entity**."

Likes 0	
Dislikes 0	

Response

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

If a Responsible Entity (RE) is found non-compliant during an audit due to ambiguous and non-quantifiable standard language, the fines could result in money being spent paying a fine that would negatively impact security elsewhere through no fault of the RE.

“100 percent coverage is not required” is ambiguous, so compliance would be met if 99.9 % coverage were achieved, and it would also be achieved at 10% IF the collection methods provide security value to address the “perceived risks”.

It doesn’t matter if the RE has 100% coverage if the RE does not “perceive” any risk or does not know how it is defined or measured. Likewise, if the RE only has 10% coverage.

What is the intention of the regulation? A RE could log every single bit of every communication and alert on every single ‘anomalous’ behavior and if the RE is not “perceiving” a risk based on some objective measurement methodology or standard, the RE is neither reducing risk nor being compliant.

Since “perceived risks” does not appear to be in the NERC Glossary of Terms, how should it be defined, and whose, or what, perception is the standard by which the compliance is measured? By the RE’s, the auditor’s or the industry, or maybe it could be any of them? This should be better defined.

We do not provide any language modifications and recommend the SDT completely review this requirement part to develop minimum quantifiable measures for compliance and utilize existing glossary terms or develop glossary terms that can be used for this requirement.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

This requirement should be broken down into two parts. One for identifying applicable network communications, and the other for identifying monitoring methods.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM

Answer	No
Document Name	

Comment

Black Hills Corporation does not fully support the proposed language. Black Hills Corporation agrees with the comments provided by EEI, "EEI does not fully support the currently proposed language for both the Applicability Section and Requirements. Relative to the Applicability Section, "access control" is insufficiently narrow and should be replaced with authentication control to more clearly define the desired scope. Additionally, the statement "100 percent coverage is not required" is too ambiguous and may create unintentional compliance expectations for registered entities. This statement should be deleted, and the last sentence should be expanded to include the statement "as determined by the responsible entity." See the proposed changes in boldface below:

Applicable Systems

High Impact BES Cyber Systems and their associated:

1. EACMS that perform **authentication** *(not "access"*) control functions;
2. PACS that rely upon EACMS that perform **authentication** *(not "access"*) control functions; and
3. PCA.

Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:

1. EACMS that perform **authentication** *(not "access"*) control functions;
2. PACS that rely upon EACMS that perform **authentication** *(not "access"*) control functions; and
3. PCA.

Requirements Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network **communications (excluding communications between ESPs)**. *(remove "100 percent coverage is not required.")* Collection methods should provide security value to address the perceived risks**, as determined by the responsible entity**."	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E does not believe the intent is clear for Part 6.1. PG&E recommends in addition to the "100 percent coverage not required", an additional clause be added that this should be a risk-based approach, as determined by the Responsible Entity.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
The language in this question is indicative of the drafting team's intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility ("100 percent coverage is not required") leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity" in place of the 100% statement as more consistent with the expressed intent. Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome.	
Likes 0	
Dislikes 0	
Response	

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA recognizes and appreciates the SDT's effort to allow Registered Entities (RE) to make their own risk-based determinations. BPA recommends that the current requirement language needs further refinement to clarify the intent. Ambiguity opens REs to subjective criticism from auditors, which in this case could be about what percentage they cover and what they consider anomalous activity. BPA suggests that R6.1 be rewritten to more clearly specify the requirement, such as "Use a risk-based assessment methodology to identify network data collection locations…" Language used elsewhere in the CIP Standards, such as "as determined by the Registered Entity", could strengthen the position that the REs are empowered to set their own risk acceptance strategy, risk mitigation, etc. BPA also suggests the final sentence ("100 percent coverage is not required…") could be incorporated into the Technical Rationale rather than the requirement.	
Likes 0	
Dislikes 0	
Response	

Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	

It is clear that 100% coverage isn’t required, but what provides “security value” and is considered “critical” isn’t. A guidance document is required. How can an auditor or entity determine they did enough? There should be a guidance document to help both the entities and auditors feel confident they are compliant with the new requirements.

It is clear that 100% coverage isn’t required, but what provides “security value” is not. If the intent is for each responsible entity to perform an assessment of their applicable CIP network communications and determine what is most critical to monitor, then that should be explicitly stated in the standard.

Please clarify what a CIP network interface is. Is this supposed to be data collection points? The minimum coverage should be defined to avoid any confusion.

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

As written, R6 P1 is vague and will cause significant disagreement between entities as to what is considered sufficient “methods” to determine what must be collected. There is no existing standard within the cyber security practice on what precisely would constitute an effective level of data collection. While the drafting team states in the Technical Rationale that “Regional Entities would require too much INSM collection and force entities to move resources from other effective cybersecurity detection systems such as SIEM and endpoint monitoring to INSM collection”, nothing about the standard itself places limits on interpretation by the RE such that what becomes deemed acceptable during audits is de facto direction by what the RE’s want. For example, if during implementation it is determined that coverage of a selection of key devices is most appropriate and such selection of devices represents 75% of devices within a network because that is assessed to be the correct level of monitoring in a method, what constrains the RE from declaring the analysis to be insufficient?

In the Technical Rationale on page 8, it refers to examples of determining “assessment”. However, the items listed as examples are not assessment tools to drive determination of what, precisely, should be collected at a per-packet level. Use of the MTIRE ATT&CK Framework is simply a taxonomy to “talk” about different stages of a cyber-attack and, notably, how to associate those terms with documentation. Two organizations using the ATT&CK framework will have substantively different interpretations of what a taxonomy element means and how it should be used, if at all. One entity’s definition may not match an RE’s definition and thus conflict will arise during audit. The Technical Rational does not solve interpretive differences, in fact it enhances them.

Another example of the problems with interpretation and execution is table of methods on pp 9-10 and combined with the reference diagram on page 14. The references are overly simplistic and not necessarily relatable to in-the-field deployments of network infrastructure. The “data collection” is referred to as a “TAP or SPAN” off a series of various switches or, in a few cases, “Network Flow”. However, each label over-simplifies a significantly complicated series of engineering decisions. For example, most switches that are not large carrier-class devices, cannot effectively tap every single port and span/repeat those packets to another location. There are significant issues with processing power available on control planes of network devices, many of which will degrade the operational performance of devices if not carefully limited. Other proposed technologies, such as sFlow, are not security protocols. sFlow is, specifically, an industry protocol that was created to sample traffic moving through an interface for the purposes of calculating bust-based bandwidth billing (e.g., calculating the 95% percentile traffic for rate billing, etc.). The reference architecture also creates an interesting chicken-egg scenario, in combination with R6 P7, where monitoring assets will themselves become assets that require monitoring.

At the end of the day, the requirement and all associated rationale is very subjective and will lead to significant interpretive differences and clashes. If the SDT is not going to mandate 100% coverage – and all pervious CIP standards essentially require 100% coverage within a given set of “Applicable Systems” listed in the part – then the decision points need to be clear so that all entities can agree on reasonable interpretations of inclusivity within a defined set of boundaries.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NRG recommends that the SDT better define what critical aspects are required to be monitored. For instance, if security monitoring on the outer layer only is deemed sufficient, this sort of language should be explicitly prescribed within the standard. The current terminology is both ambiguous and subjective by nature, and, as such, could be interpreted in many different ways depending on the party

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NRG recommends that the SDT better define what critical aspects are required to be monitored. For instance, if security monitoring on the outer layer only is deemed sufficient, this sort of language should be explicitly prescribed within the standard. The current terminology is both ambiguous and subjective by nature, and, as such, could be interpreted in many different ways depending on the party.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Even though the Requirement states “100 percent coverage is not required”, this requirement is too subjective and open to different interpretations and implementations; this could prove difficult in providing adequate evidence in an audit. Suggested language for 6.1 is as follows: “*Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications based on the network risk as determined and documented by the Responsible Entity and per Cyber Asset or BES Cyber System capability or where technically feasible. Collection methods should provide security value to address the perceived risks.”*	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	

Answer	No
Document Name	

Comment

The language in this question is indicative of the drafting team's intent to provide needed flexibility to Responsible Entities in designing their INSM system. Our concern is that the language meant to provide that flexibility ("100 percent coverage is not required") leaves how much less than 100% is sufficient to the second-guessing of any auditor. We propose continuing the first sentence with "commensurate with network risk as determined by the Responsible Entity" in place of the 100% statement as more consistent with the expressed intent.

Also, the webinar presented on 1/3/2024 (at 1:04:30) provided additional insight on the evidencing of compliance with Part 6.1. Comments indicated that if you can identify and find malicious behavior in the network you have met the requirement. We recommend that the SDT add an example to Measure 6.1 that successful detection of attempted penetration testing can be used to demonstrate sufficiency of collection locations. Additional examples of satisfactory evidence would also be welcome.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

It is unclear what type of data is to be collected. Suggest revise to define expectations for what type of data should be collected. There is no minimum threshold for acceptable INSM coverage. Suggest revise to clearly define what type of data is to be collected, and establish a minimum threshold for what INSM coverage is acceptable. The undefined term "connection" is unclear in context. Suggest define what is meant by this term.

Consider leveraging the OSI model to clearly identify the target depth of monitoring. It is unclear what the level of information (eg Layer 2, 4, or 7) is required to be collected and stored to satisfy the requirement.

Likes 0	
Dislikes 0	

Response

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group

Answer	No
Document Name	

Comment

There are really two things being asked here: (1) perform the assessment to determine what is most critical to monitor and (2) identify the locations and methods to perform the monitoring. As written, it is not clear that both are being asked. So, this requirement either needs to be rewritten or broken up into two parts. It could be rewritten as “Assess network communications (excluding serial) between applicable Cyber Assets to determine the most critical communications and identify network data collection locations that monitor and detect for anomalous activity.”	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
The last sentence, which refers to security value to address the perceived risks, is highly vague. It is not clear how an auditor would verify what is the perception of risks for an entity or the security value.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	

Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the current language in 6.1 is clear to the intent that every network interface will not have to be monitored. Entities should consider however, that this approach will require they have a consistent rationale for what is included and be able to defend communications that fall into scope but were not selected for inclusion.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #4.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	

Answer	
Document Name	
Comment	
Texas RE agrees that under the current language 100 percent coverage is not required. Texas RE recommends, however, the language clarify and add threshold of acceptable monitoring so the standards applied and enforced consistently. Rather than mandating a specific minimum percentage, Texas RE suggests certain systems, such as operator consoles that are used to operate the Bulk Electric System, should be a mandatory inclusion within the INSM program. Alternatively, the SDT may wish to require entities to justify the parameters they have developed to meet the requirement to “[i]dentify network data collection locations and methods that provide visibility of network communications” so that the rationale for inclusion/exclusion is transparent.	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	
The standard should clearly indicate that the entity would be responsible for performing an assessment (preferably risk based) from which the most critical interfaces (chosen by the entity) will be applicable. See additional comments for more details.	
Likes 0	
Dislikes 0	
Response	

5. The Project 2023-03 SDT held extensive conversations about the term “baseline” and what alternatives there might be to avoid confusion with the term baseline used in Reliability Standard CIP-010-4, Requirement R1, Part 1.1. Ultimately, the SDT could not find a suitable alternative and believed that it should be clear that a network communications baseline would be entirely different from a software baseline used in Reliability Standard CIP-010-4. Do you agree that the SDT’s use of the term “network communications ‘baseline’” is clear in Requirement R6 Part 6.3? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	No
Document Name	
Comment	
The term baseline is appropriate because the entity is creating a baseline of the network activity, although there is room to improve the requirement. Consider rephrasing R6.3 to something like “Evaluate and create a network communications baseline using the collected data in Part 6.2.” This should adequately differentiate this baseline from the one used in the CIP-010 standard.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The undefined term “baseline” is ambiguous, and is already in use in CIP-010 in a different context. Suggest revise to define what is meant by “baseline” in this context, preferably use a different term. Identify clear retention requirements that are achievable with current marketplace offerings. For example, ISPs will leverage netflow data to maintain long term trends on interface and protocol utilization. It’s relatively low cost, and low storage requirements, yet allows for historical analysis and trending over time.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No

Document Name	
Comment	
The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3, and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish.” The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic.	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No
Document Name	
Comment	
Suggested change: “network communication baseline” to “protocol baseline”. This aligns with the various ICS and non-ICS data communication protocols that could be detected in the network environment.	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Wording of 6.3, in particular, needs to be addressed by changing the word “Document” to “Establish” or “Develop” the expected network communication baseline. This will give the Responsible Entity the flexibility in their evaluation of the collected data in how they determine an expected network communication baseline.	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
While NRG understands the SDT's intent on the "network communication baseline" terminology, we recommend providing some additional examples of evidence within the "Measures" section of the standard to help better define the proposed "baseline" term and ultimately make it a bit less ambiguous. Another option of the SDT would be to formally define the "network communication baseline" term and include it in the NERC Glossary of Terms.	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
While NRG understands the SDT's intent on the "network communication baseline" terminology, we recommend providing some additional examples of evidence within the "Measures" section of the standard to help better define the proposed "baseline" term and ultimately make it a bit less ambiguous. Another option of the SDT would be to formally define the "network communication baseline" term and include it in the NERC Glossary of Terms.	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
The use of “baseline”, while understandable, will still create overloading of the word as it’s already extensively used in CIP-010 and, by implicit reference, CIP-007 R1 and R2. Suggest the following language for Requirements: Record, evaluate and pattern the collected data sufficiently such that significant deviations from historical records are detectable.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
The term is clear; however, what it consists of should be specified as it is in CIP-010-4 R1.1. Consideration for adding a new NERC term, such as “Network Communication Baseline,” to the glossary should be made. The minimum frequency of evaluation should be included, or if the expectation is real-time, that should be stated. This specific requirement is unclear. Could it be that this is a request for entities to document expected communications between assets in the environment? This may be an overkill as CIP-010-4 already adequately covers assets baseline and change management. The use of software may be necessary to determine the baseline communications amongst assets, but this may not be affordable for many (smaller) entities. The possibility of removing this requirement should be considered.	
Likes 0	
Dislikes 0	
Response	

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3, and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish.” The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic. This change supports the use of vendor proprietary technology for network traffic baselines, where the product may not be able to “output” a baseline but uses trending and comparisons to detect anomalies.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E believes this requirement will be difficult to fulfill, as we don’t know what a network communication “baseline” will look like. How do we document a baseline? It is also not sustainable to maintain a static documented baseline. PG&E believes this will most likely be defined by the security vendor	

that is being used and probably will not be publicly available (and will probably be internal configuration settings rather than a written baseline). PG&E also believes this requirement may not be feasible or necessary, given the logging and analysis requirements in other R6 sections**.**	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	No
Document Name	
Comment	
Black Hills Corporation does not support the Requirement 6, 6.3 as currently written. Black Hills Corporation agrees with the comment provided by EEI, “EEI does not support the Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a** (*remove "Evaluate the collected data to document the expected"*) network communication baseline **through methods that record normal traffic to network assets and are continuously updated**.”	
Likes 0	
Dislikes 0	
Response	
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	
The term baseline can and will be confusing – since CIP-010 use the term “baseline”, There should be a different term to be used instead of using the term “network communications baseline”. The term ‘baseline’ already being widely used and understood across industry to refer to a software baseline in CIP-010 R1. Baseline is not sufficiently defined, and many would interpret this to imply a point in time capture of desired system state. The requirement states the baseline should be derived from evaluation of the collected data. However, collected data may differ considerably from the “Expected network communication” as documented in application/OS requirements and could lead to anomalous traffic being included within the baseline. The recommendation would be to specifically define both “network communications baseline” and “software baseline” separately in the NERC glossary of terms.	
Likes 0	

Dislikes 0

Response

Byron Booker - Oncor Electric Delivery - 1

Answer No

Document Name

Comment

Oncor stands in agreement with comments made by by EEI that states:

"EEI does not support Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface:

Develop and establish a Evaluate the collected data to document the expected network communication baseline **through methods that record normal traffic to network assets and are continuously updated**."

Likes 0

Dislikes 0

Response

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

Answer No

Document Name

Comment

Tri-State agrees with MRO provided comments:

"The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3 and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish”. The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which is evaluates all network traffic."

Likes 0

Dislikes 0

Response

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 that the Standards Drafting Team simply remove the word “baseline” and we propose the following language for Requirement R6 Part 6.3. “Implement methods to evaluate collected data to establish the expected network traffic.”	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
We agree that the concept of a network baseline makes sense but do have concerns that the diversity with which entities might construct these baselines . We support EEI proposed language to include “through methods that record normal traffic to network assets” at the end of 6.3 to encourage alignment on the expected outcome. It may be necessary to specify minimum elements for collection.If the term baseline is problematic, it could be removed all together in 6.3 if adequately specificity is given.	
Likes 0	
Dislikes 0	
Response	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource supports the comments of EEI.	

Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Cleco agrees with EEI comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	
NEE supports EEI comments: " EEI does not support Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a Evaluate the collected data to document the expected** network communication baseline **through methods that record normal traffic to network assets**. "	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	

Propose changing the term “document” to “establish." to enable demonstration that a baseline has been established, but not require documentation. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

It would be helpful to have particular aspects of a network communication baseline be clearly defined in the standard (similar to a baseline in CIP-010 R1.1). Maybe some wording like “including but not limited to”, so that utilities have some network communication baseline structure to work off of as recommended by NERC. This would clarify the compliance expectation when providing evidence for network communication baseline.

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 3

Answer	No
Document Name	

Comment

If the term “network communications baseline” is to remain undefined by NERC, then the requirement should include language directing the entity to define what constitutes the “expected network communication baseline” that is being documented and monitored. 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”. This ensures that monitoring and evaluation of deviations is occurring against a well-defined standard, and reduces compliance evaluation ambiguity for the entities both internally and externally.

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP does not agree with the SDT's use of the term "network communications baseline" in Part 6.3. With the industry-approved, virtualization-related changes from NERC Project 2016-02 including the removal of the term "baseline" from the currently enforceable version of CIP-010, the term "baseline" is not anticipated to be used in the future enforceable NERC CIP requirements. In addition, the SDT should consider adding "application flows" as part of the requirement language to help this requirement its overall intent. SPP proposes the following language for Part 6.3: *Evaluate the collected data to document the expected application flows and network communications.* SPP also supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
There will continue to be confusion about what network communication baseline means. Adding examples to what constitutes a network communication baseline would help (netflow, pcap, etc)	
Likes 0	
Dislikes 0	
Response	
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	

It is unclear about the impactful relationship between the CIP-010 baseline and the CIP-007 network baseline.

The term is clear; however, what it consists of should be specified as it is in CIP-010-4 R1.1. Consideration for adding a new NERC term, such as "Network Communication Baseline," to the glossary should be made. The minimum frequency of evaluation should be included, or if the expectation is real-time, that should be stated.

This specific requirement is unclear. Could it be that this is a request for entities to document expected communications between assets in the environment? This may be an overkill as CIP-010-4 already adequately covers assets baseline and change management.

The use of software may be necessary to determine the baseline communications amongst assets, but this may not be affordable for many (smaller) entities. The possibility of removing this requirement should be considered.

Likes 0	
Dislikes 0	

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer	No
Document Name	

Comment

"See comments submitted by the Edison Electric Institute"

Likes 0	
Dislikes 0	

Response

Whitney Wallace - Calpine Corporation - 5

Answer	No
Document Name	

Comment

There will continue to be confusion about what network communication baseline means. Adding examples to what constitutes a network communication baseline would help (netflow, pcap, etc)

Likes 0	
Dislikes 0	

Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
It is unclear about the impactful relationship between the CIP-010 baseline and the CIP-007 network baseline. The term is clear; however, what it consists of should be specified as it is in CIP-010-4 R1.1. Consideration for adding a new NERC term, such as “Network Communication Baseline,” to the glossary should be made. The minimum frequency of evaluation should be included, or if the expectation is real-time, that should be stated. This specific requirement is unclear. Could it be that this is a request for entities to document expected communications between assets in the environment? This may be an overkill as CIP-010-4 already adequately covers assets baseline and change management. The use of software may be necessary to determine the baseline communications amongst assets, but this may not be affordable for many (smaller) entities. The possibility of removing this requirement should be considered.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
Ameren would like more clarification around the term "baseline."	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	

Comment

Avista agrees with EEI’s comments: EEI does not support the Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface:

Develop and establish a Evaluate the collected data to document the expected network communication baseline **through methods that record normal traffic to network assets and are continuously updated**.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

From the NERC meeting which took place on 1/3/2024, the concept of a baseline was clarified to not be a point-in-time list, a spreadsheet, etc. but more of an expected network communication *behavior* and *functionality* against which the collected data can be evaluated. If this is the case, the Requirement should not have a term (baseline) that is to be interpreted. The focus is on evaluating expected network behavior against anomalous activities.

Proposed language: “Evaluate the collected data to maintain the expected network behavior.”

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI does not support Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface:

Develop and establish a network communication baseline **through methods that record normal traffic to network assets**.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the comments as provided by EEI and NSRF.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	

Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	No
Document Name	
Comment	
Avista agrees with EEI’s comments: EEI does not support the Requirement 6, part 6.3 as currently written because the requirement is not clear and is not a risk-based requirement. To address our concerns, we suggest the following changes in boldface: **Develop and establish a** network communication baseline **through methods that record normal traffic to network assets and are continuously updated**.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	

Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
The term “baseline” is confusing given its well-established meaning within the context of CIP-010. An alternative term should be used and defined (e.g., “Traffic Profile” or “Expected Traffic”).	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
The term "Network communication 'baseline'" lacks clarity and introduces significant potential for confusion, particularly given its distinct usage in CIP-010. Consequently, it is advisable to refrain from employing "baseline" in the context of CIP-007 to avoid misinterpretation. The proposed Measures incorporate the term "expected network communications," which we believe adequately characterizes the information sought. However, the Measure itself falls short in delineating the specifics of the anticipated evidence. A record encompassing "expected network communications" is likely to amass a volume that surpasses human readability. This raises the pertinent question: What elements are anticipated to be included in this record? Does it necessitate an exhaustive enumeration of every conceivable endpoint and each individual protocol? Clarification is essential for a comprehensive understanding of the proposed Measure.	
Likes 0	
Dislikes 0	
Response	

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The term “baseline” is confusing given its well-established meaning within the context of CIP-010. An alternative term should be used and defined (e.g., “Traffic Profile” or “Expected Traffic”).	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
More information is needed to determine what would be a suitable baseline. Does an entity have to provide documentation from vendors to support the baseline? Without more information on what constitutes a baseline and what evidence is required to justify the baseline it leaves too much open to interpretation by an auditor. Entities will vary on the methodology used to determine their baselines and this makes it hard for an auditor.	
Likes 0	
Dislikes 0	

Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not agree that the term “network communications baseline” is clear in Requirement R6, Part 6.3. CEHE believes that the “network communications baseline” term implies a known “good” and “bad” set of behaviors, but network activity is very often not as easily categorized nor explainable. It is often very difficult to determine when an anomaly is occurring based on a baseline criterion but is more of a judgement call that develops over time. CEHE recommends revising the requirement to include a frequent evaluation of entities network communications, as determined by the Registered Entity. The requirement should not suggest that there is a clear criteria or baseline that governs the results of the evaluation.	
Likes 0	
Dislikes 0	
Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern Company does not agree with R6 Part 6.3 as currently written. These requirement parts (6.2-6.5) are detailing a procedural “how” of meeting a security objective, which could be combined into “implement a process to monitor the identified collection points for anomalous activity including connections, devices, or communications” with response criteria and processes. A baseline can be a stated measure of how the entity determines anomalous activity. Southern Company suggests making the standard more future-proof, it needs to be more objective as security principles such as Zero Trust are incorporated with increasingly more communications in device to device encrypted tunnels thus reducing the usefulness of "on the wire" monitoring over time. Virtualization, containerization, micro-segmentation, etc. are all variables in how, and at what level, security monitoring may be best performed in the timeframe of this standard's implementation plan. Currently the language requires the baseline be built only from monitoring the network. We suggest the standard require what the entity is to accomplish, not procedural steps of how to “do” INSM with today’s tools. That is better left to Implementation Guidance or Technical Rationale and could simplify this requirement from its current 7 step process.	
Likes 0	
Dislikes 0	
Response	

Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree that the term “network communications baseline” is clear in Requirement R6, Part 6.3. SIGE believes that the “network communications baseline” term implies a known “good” and “bad” set of behaviors, but network activity is very often not as easily categorized nor explainable. It is often very difficult to determine when an anomaly is occurring based on a baseline criterion but is more of a judgement call that develops over time. SIGE recommends revising the requirement to include a frequent evaluation of entities network communications, as determined by the Registered Entity. The requirement should not suggest that there is a clear criteria or baseline that governs the results of the evaluation.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
The problem is not with the term “baseline” but the requirement to “document” it. Webinar slide 18 showed what is and is not regarded as a baseline for the purpose of 6.3, and we agree. The problem is that documenting the baseline as supporting evidence would have to take the form of what a baseline is not. We propose changing the term “document” to “establish.” The Measure should be re-written to simply allow for demonstration that a baseline has been established. Examples could include network files containing baseline information, or vendor documentation indicating the INSM does establish a baseline of expected network communications against which it evaluates all network traffic.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	No
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	No
Document Name	
Comment	
Considering the 2016-02 SDT CIP-010 R1 language has moved away from documenting baselines and leveraging automation, the 2023-03 SDT should adopt a similar approach from - ‘Evaluate the collected data to document the expected network communication baseline.’ To - ‘Evaluate the collected data to establish the expected network communications.’	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes

Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
NST sees no problem with distinguishing network traffic baselines from endpoint device configuration baselines. We also note that if the most recent modifications to CIP-010 made by the Project 2016-02 SDT are approved by the NERC Board and by FERC, Responsible Entities will no longer be required to maintain configuration baselines as evidence of compliance with that Standard, which will further reduce the risk of confusion.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	

Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees that the use of the term “network communications baseline” in Requirement R6, sub-requirement 6.3.	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE agrees that network communications baseline is clear in Requirement R6 Part 6.3. If the SDT wishes to avoid the use of the word ‘baseline’ in this requirement Texas RE proposes any of the following requirement language alternatives:

- Evaluate the collected data to document the expected network communications profile.
- Evaluate the collected data to document the expected network communications traffic.

• Evaluate the collected data to document the expected network communications traffic pattern(s).	
Likes 0	
Dislikes 0	
Response	

6. The Project 2023-03 SDT held extensive discussions regarding the use of the term “anomalous.” The SDT did not intend for responsible entities to use only signature-based tools to detect suspicious activity, and thus, the use of “anomalous” was descriptive of approaches that looked at a normal network communications baseline and identified deviations. The intent was to not only discover known malicious communications, but to identify unusual communications that need to be investigated, and the SDT decided that the term “anomalous” was the appropriate term to use to describe that methodology. Do you agree that that the term “anomalous” effectively describes those methodologies? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We understand the reasons presented for using the term “anomalous,” but we are concerned that tying requirements to so broad a term greatly increases compliance responsibilities relative to the term “anomalous network activity indicative of an attack in progress” used in the FERC order. Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to “anomalous network activity indicative of an attack in progress” should be subject to compliance.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	

WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Anomalous traffic may be expected from the baseline during outage or troubleshooting or testing, and it may be impossible to capture them in the network baseline. The standard should have verbiage to exclude those scenarios.	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	No
Document Name	
Comment	
AZPS believes that “anomalous activity” is ambiguous. We recommend language similar to the question above “deviations from a normal network communications baseline”	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

Minnesota Power supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support comments as provided by the NSRF.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
Some network anomalies are expected and are difficult to always predict. How do we account for outages, upgrades, testing, etc.	
Likes 0	
Dislikes 0	
Response	
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	

Some network anomalies are expected and are difficult to always predict. How do we account for outages, upgrades, testing, etc.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	No
Document Name	
Comment	
The term “anomalous,” is too vague and covers too many potential activities. The SRC recommends using the phrase from FERC Order No. 887: “anomalous network activity indicative of an attack in progress” as detailed below: *CIP-007-X Table R6 – INSM: Part 6.4 Requirements* *Deploy one or more method(s) to detect anomalous* ***network*** *activities* ***indicative of an attack in progress****, including connections, devices, and network communications using data from Part 6.2.*	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
While SPP does not have concern with the term “anomalous”, SPP believes the current purposed language is beyond the scope of FERC Order 887, which states “anomalous network activity indicative of an attack in progress.” SPP proposes updating the language in Parts 6.1, 6.4, 6.5, and 6.6 to include the language “anomalous network activity indicative of an attack in progress.”	
Likes 0	
Dislikes 0	
Response	

Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	No
Document Name	
Comment	
If the term “anomalous” is to remain undefined by NERC, then the requirement should include language directing the entity to define the anomalous activity they are monitoring. For example, language similar to the CIP-008 R1.2.1 requirement that directs entities to “include criteria to evaluate and define attempts to compromise”. If entities are allowed the latitude to define criteria for anomalous events to report to E-ISAC in CIP-008, they should be afforded that opportunity for anomalous events in this standard. This also reduces compliance evaluation ambiguity for the entities both internally and externally.	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to “anomalous network activity indicative of an attack in progress” should be subject to compliance.	
Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Reclamation recommends where possible align proposed terms with NIST current definitions.

NIST definition examples:

Anomaly - Condition that deviates from expectations based on requirements specifications, design documents, user documents, or standards, or from someone's perceptions or experiences.

Behavioral Anomaly Detection - A mechanism providing a multifaceted approach to detecting cybersecurity attacks.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

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

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

While Dominion Energy understands why the term "anomalous" was chosen by the SDT, we recommend additional clarifying language be added to make it clear that stakeholders, who have the best understading of their networks, are responsible for determing what is anomalous. We recommend the addition of the phrase "as determind by the Registered Entity" be added to qualify anamolous.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Tri-State recoomends using the words normal or abnormal in place of anomalous.

Likes 0	
Dislikes 0	

Response

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

The recommendation would be not to use the word “anomalous” at all. Recommend the use of “unusual communications that need to be investigated” instead. Using the terms “unusual communications that need to be investigated” removes the ambiguity of what an entity would define as “anomalous”.

If the word “anomalous” is used in the standard, it must be defined in the glossary of terms with the definition specific to the SDT’s intent of its definition, namely, “unusual communications that need to be investigated” since the dictionary definition of the word anomalous is, “deviating from what is standard, normal, or expected.”

This definition would allow for entities to consider an “unusual communications that need to be investigated” event as “normal” or “expected” and the expected understanding of the word anomalous in this context and requirement would be lost.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The term “anomalous” is too broad. We suggest focusing on wording similar to “deviations from the network communications baseline.”	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
SDT should consider defining anomalous to avoid any confusion for entities. See additional comments for more details.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E believes the term “anomalous” is vague. PG&E recommends using the phrasing from FERC Order 887 “anomalous network activity indicative of an attack in progress.”	
Likes 0	
Dislikes 0	
Response	

Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	No
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group	
Answer	No
Document Name	
Comment	
Manitoba Hydro understands the reasons presented for using the term “anomalous,” but we are concerned that tying requirements to so broad a term greatly increases compliance responsibilities relative to the term “anomalous network activity indicative of an attack in progress” used in the FERC order. Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to “anomalous network activity indicative of an attack in progress” should be subject to compliance. This clearly defines the scope of the standard, for example if a product detects anomalies related to system network communication malfunctions these may be useful to an entity but out of scope of compliance. Leaving the term “anomalous” in continues to differentiate between detected “anomalous” activity and a confirmed attack in progress.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	

The use of “anomalous” is fine however suggest including “potentially” and to align with proposed language from proposed R6P2: Deploy one or more method(s) to detect potentially anomalous activities, including connections, devices, and network communications using data from Part 6.2	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
MRO NSRF understands the reasons presented for using the term “anomalous,” but we are concerned that tying requirements to so broad a term greatly increases compliance responsibilities relative to the term “anomalous network activity indicative of an attack in progress” used in the FERC order. Responsible Entities should not be administratively burdened in satisfactorily evidencing the collection and analysis of non-threat network activity. Only deficiencies in detecting, analyzing, and responding to “anomalous network activity indicative of an attack in progress” should be subject to compliance.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The undefined term “anomalous” is ambiguous and may create confusion for both entities and the CEA to determine what specific activities are included. Suggest revise to provide a clear criteria for determining what activities are “anomalous” that is consistent with existing CIP-008 obligations.	
Likes 0	
Dislikes 0	
Response	

Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	No
Document Name	
Comment	
The term “anomalous” is not specific enough. It would be clearer to build on the language used in R6.3. In R6.3, we essentially determine what is not “anomalous” (e.g., what is acceptably part of the network communications baseline). Consider rephrasing as “to detect activity that deviate from the network communications baseline identified in Part 6.2” or similar. This clarifies the intent, eliminates the need to include “anomalous”, enhances cybersecurity by converting the “black list” to a “white list” monitoring method, and reinforces the importance of the communications baseline throughout R6.	
Likes 0	
Dislikes 0	
Response	

Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	

Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Southern Company agrees with the comments by EEI.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon is of the opinion that the term “anomalous” is sufficiently clear to describe the methodologies.	
Likes 0	
Dislikes 0	

Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI is of the opinion that the term “anomalous” is sufficiently clear to describe the methodologies.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF agrees with use of the term “anomalous”.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	Yes
Document Name	
Comment	
One potential issue NST does see here arises from the SDT's assertion, in the draft Technical Rationale document, that a baseline is "Continuously updated by a computer" and not a "Point-in-time list." We believe these assertions are incorrect. Merriam-Webster's online dictionary defines "baseline" as, "a usually initial set of critical observations or data used for comparison or a control." Similarly, several references NST consulted define network baselines as "snapshots" that can be used to set expectations about traffic types, volumes, sending and receiving devices, etc. during some period of time (e.g., weekdays from 8 AM to 6 PM local time). While we certainly agree baselines	

should be updated periodically, we are hard-pressed to understand how anomalous traffic can be detected if a baseline that is intended to represent "expected" traffic is being ***continuously*** updated.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: “ EEI is of the opinion that the term “anomalous” is sufficiently clear to describe the methodologies. “	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees that the term "anomalous" is appropriate.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	

Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

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	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

7. The Project 2023-03 SDT tried to clarify that the process to determine appropriate action regarding anomalous activity in Requirement R6, Part 6.4 occurred prior to escalation and potential initiation of a responsible entity's CIP-008 process. Do you agree that the SDT was clear that this occurs before the determination of a Cyber Security Incident? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	No
Document Name	
Comment	
It would be clearer to use language in R6.5 like that of CIP-005-7 R1.5 "Have one or more methods". Also, as stated in question 6, not using the term "anomalous" would be beneficial here. Consider language like "Have one or more method(s) to evaluate activity that deviates from the baseline identified in Part 6.2." This approach supports the ability to evaluate the finding before initiating a CIP-008 Cyber Security Incident determination while maintaining continuity with other existing standards.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The undefined term "anomalous" lacks the clarity to distinguish between activities addressed in Part 6.4 and activities that should initiate a CIP-008 process.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	

It is clear that Part 6.4 detection of anomalous activity precedes Part 6.5 evaluation. The webinar made it clear that CIP-007 Part 6.5 will feed into CIP-008 when the evaluation warrants. What is needed is language protecting Responsible Entities from double jeopardy such that any violation of CIP-007 R6.5 does not result in a concurrent CIP-008 violation, and vice versa.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee's comments.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
As above, suggest the inclusion of "potentially" and to outline that anomalous may not be malicious: One or more process(es) to evaluate potentially anomalous activity identified in Part 6.4 to determine appropriate action including, but not limited to, adjustments to the traffic patterns from Part 6.2 or investigation as a potential security incident.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	

Answer	No
Document Name	
Comment	

It is clear this happens prior to escalation to the CIP-008 process. Without a frequency on verifying the baseline, the anomalous activity might not trigger promptly enough.

There is no wording stating specifically that escalation and potential initiation of a responsible entity's CIP-008 process is the appropriate action if a legitimate threat is detected.

Likes 0	
Dislikes 0	
Response	

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	No
Document Name	
Comment	

It is clear that Part 6.4 detection of anomalous activity precedes Part 6.5 evaluation. The webinar made it clear that CIP-007 Part 6.5 will feed into CIP-008 when the evaluation warrants. To clarify the link the requirement could be re-worded:

One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine if it is related to a Cyber Security Incident.

The measures lists potential evidence as “documentation of responses to detected anomalies”. Manitoba Hydro suggests removing this from the measures to focus on evidence related to having the process documented. When systems are first put in they may generate a lot of alerts before they are “tuned” and evidence of review of every single alert may be burdensome without any practical security value.

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	
Texas RE recommends the following requirement language: One or more process(es) to evaluate anomalous activity identified in Part 6.4 as a potential Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
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	
It is not clear how to determine when action is required.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No
Document Name	

Comment	
I believe this question may refer to an older version of the draft standard. This question makes more sense regarding Part 6.5, and the INSM drafting team outreach presentation discusses CIP-008 in the context of Part 6.5. However, the actual language of Part 6.5 does not reference CIP-008, and therefore any anomalous activity could be interpreted as an attempt to compromise and/or an actual compromise that triggers the requirements of CIP-008. It isn't enough to include the SDT's intention in an outreach presentation - if it isn't in the standard, an auditor will not consider it.	
Likes 0	
Dislikes 0	
Response	
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	
This question appears to reference CIP-007-X Requirement R6 Part6.5 and this question is not clear and not very well defined. We recommend changing Requirement R6 Part 6.5 to state: “Implement methods to evaluate anomalous activity identified in Part 6.4.”	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
In 6.5 Duke Energy recommends additional language to clarify the intent of the evaluation. *One or more process(es) to evaluate anomalous activity identified in Part 6.4 for indications of an attack in progress, and if such indications are detected, to determine appropriate action.*	
Likes 0	
Dislikes 0	

Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
As currently written, neither R6 nor any of its parts say anything about CIP-008. NST suggests language such as, "Develop and deploy methods to detect anomalous network activity and to identify potential Cyber Security Incidents."	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends adding additional language to CIP-007 R6 to clarify that this occurs before the determination of a Cyber Security Incident.	
Likes 0	
Dislikes 0	

Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
Suggest including language protecting Responsible Entities from double jeopardy such that any violation of CIP-007 R6.5 does not result in a concurrent CIP-008 violation, and vise versa.	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The language wasn’t that prescriptive and appeared to allow the company to determine the correct course and sequence of actions based on the event. No further clarity is needed.	
Likes 0	
Dislikes 0	
Response	
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	
Answer	No
Document Name	
Comment	

Since the requirement language in R6 Part 6.5 does not mention CIP-008 or Cyber Security Incidents, there is no relationship established between R6 Part 6.5 and CIP-008 or a Cyber Security Incident. Additionally, the requirement language may fall within the current processes identified for Cyber Security Incident Response by the Responsible Entity, and could cause multiple response paths to be created.

Likes 0	
Dislikes 0	

Response

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

The appropriate action regarding anomalous activity should not always be construed as prerequisite of CIP-008. Recommend that 6.5 references to evaluate what is detected as opposed to “identified”.

It is clear this happens prior to escalation to the CIP-008 process. Without a frequency on verifying the baseline, the anomalous activity might not trigger promptly enough.

There is no wording stating specifically that escalation and potential initiation of a responsible entity’s CIP-008 process is the appropriate action if a legitimate threat is detected.

Likes 0	
Dislikes 0	

Response

Whitney Wallace - Calpine Corporation - 5

Answer	No
Document Name	

Comment

The language wasn’t that prescriptive and appeared to allow the company to determine the correct course and sequence of actions based on the event. No further clarity is needed.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	No
Document Name	
Comment	
The appropriate action regarding anomalous activity should not always be construed as prerequisite of CIP-008. Recommend that 6.5 references to evaluate what is detected as opposed to “identified”. It is clear this happens prior to escalation to the CIP-008 process. Without a frequency on verifying the baseline, the anomalous activity might not trigger promptly enough. There is no wording stating specifically that escalation and potential initiation of a responsible entity’s CIP-008 process is the appropriate action if a legitimate threat is detected.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	

The requirement appears to mean that analysis is required prior to the determination of a Reportable Cyber Security Incident or an attempt to compromise. To increase clarity, it may be beneficial to add “in an ongoing manner” to the end of the requirement.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
As written, the requirement could potentially result in a self-report if any “anomalous activity” occurs and is not detected.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
The requirement appears to mean that analysis is required prior to the determination of a Reportable Cyber Security Incident or an attempt to compromise. To increase clarity, it may be beneficial to add “in an ongoing manner” to the end of the requirement.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	

WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
The use of the term “anomalous’ in Requirement R6, Part 6.4 is fine, but this starts to overlap with an entity’s CIP-008 Incident Response Program”. An entity already has definitions for attempt to compromise in the Incident Response Plan and if “anomalous” activity is detected it should refer back to its incident response plan. Just because an entity detects anomalous activity and they refer to their incident response plan it does not mean it is a Cyber Security Incident, it just needs to be investigated.	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not believe that Requirement R6, Part 6.4 nor Requirement R6, Part 6.5 addresses the process of evaluating anomalous activity prior to escalation and potential initiation of a responsible entity’s CIP-008 process. Requirement R6, Part 6.4 requires methods to detect anomalous activity. Requirement R6, Part 6.4 does not address investigation or evaluation. Requirement R6, Part 6.5 requires a process to evaluate the anomalous activity identified in Requirement R6, Part 6.4. SIGE suggests including “prior to the initiation of a responsible entity’s CIP-008 process” in Part 6.5 so that the new requirement would read, “One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action, prior to the initiation of a responsible entity’s CIP-008 process.”	
Likes 0	
Dislikes 0	
Response	

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
It is clear that Part 6.4 detection of anomalous activity precedes Part 6.5 evaluation. The webinar made it clear that CIP-007 Part 6.5 will feed into CIP-008 when the evaluation warrants. What is needed is language protecting Responsible Entities from double jeopardy such that any violation of CIP-007 R6.5 does not result in a concurrent CIP-008 violation, and vice versa.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA suggests that clear language be added to tie R6.5 and/or R6.6 to CIP-008 in coordination with the Project 2022-05 drafting team. How a hand-off from a suspected malicious event is directed into a reporting requirement for “attempts to compromise” is under discussion under Project 2022-05. Ambiguity around analyzing whether an event is a security incident, what threshold for reporting such an incident might need, and the process to tie it into incident response activities including mitigation has the potential for creating duplicative and distracting requirements. BPA recommends the SDT change the word “Deploy” to “Utilize”. BPA believes deployment implies implementation of new technologies not currently in the Registered Entity’s environment.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees that the DT was clear that Part 6.4 would occur before determining if a Cyber Security Incident had occurred.	

Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: “ EEI agrees that the language proposed in Requirement R6, Part 6.4 is sufficiently clear.“	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	

Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
SPP agrees that the process to determine appropriate action regarding anomalous activity in Part 6.4 occurs prior to escalation and potential initiation of a Responsible Entity’s CIP-008 process (i.e., before the determination of a Cyber Security Incident). However, there appears to be a typographical error in this question. SPP believes the SDT intended to reference Part 6.5 since it is more appropriate for the content of this question.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes

Document Name	
Comment	
The NAGF believes that the process has been adequately clarified.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the language proposed in Requirement R6, Part 6.4 is sufficiently clear.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
The process is clear as laid out in 6.4 detection and 6.5 evaluation. It is only this question that is confusing, referencing only 6.4 in a discussion about the 6.5 evaluation.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes

Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon agrees that the language proposed in Requirement R6, Part 6.4 is sufficiently clear.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	Yes

Document Name	
Comment	
Southern Company agrees with the comments by EEI.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

8. Throughout proposed Requirement R6, the Project 2023-03 SDT tried to create a requirement that was objective based and allow latitude for various INSM methodologies and technologies to be used now and in the future. Do you agree that the SDT was successful in this endeavor? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company agrees that the language in Requirement R6 is objective based and allows latitude for various entity INSM methodologies and technologies, noting our suggested changes outlined in Question #5 (above).

Likes 0	
Dislikes 0	

Response

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CEHE believes that the requirement itself is objective- based; however, the scope described in the CIP-007-X Technical Rationale is in broad prescriptive terms. The Technical Rationale should clearly state that it does not determine the scope.

Likes 0	
Dislikes 0	

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

There doesn’t appear to be much latitude in how to implement methodology.

Likes 0	
Dislikes 0	

Response

Katrina Lyons - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC believes requirement part 6.3, which mandates the evaluation of collected data to document the expected network communication baseline, poses a limitation on certain technology platforms, notably Intrusion Detection Systems (IDS). This constraint arises from the inherent characteristics of certain IDS technologies, which may not facilitate the documentation of an expected network communication baseline. In specific instances, certain IDS technologies generate alerts predicated on Indicators of Compromise (IoC) signatures without establishing a network model for triggering alerts based on anomalous behavior against the established network communication model.

The FERC order specifically identifies IDS as a potential technology for implementing Internal Network Security Monitoring.

In Part 6.1, GSOC recommends aligning the use of terms like "Cyber Asset" in Requirement language with the terminology used in the recently approved versions of the Standard drafted by Project 2016-02. Specifically, in that version of the Standard, the coverage would only extend to a physical Cyber Asset, overlooking a Virtual Cyber Asset.

In Part 6.1, the exclusion labeled "(excluding serial)" lacks clarity, especially when contemplating the utilization of serial-based network communications like T1's. GSOC suggests refining this exemption to enhance clarity, citing other instances in the Standards where exclusions for this type of communication are present or possibly utilizing routable communications.

In Part 6.2, GSOC finds it unclear what type of log data is required and the necessary retention policy to comply with the current wording. GSOC proposes incorporating objective language that allows entities to define an appropriate retention period for the log data.

Concerning Part 6.3, GSOC notes that the Requirement lacks sufficient clarity regarding what constitutes an evaluation. It merely states that the entity should look for deviations from expected network communications without specifying what should be included in expected communications.

GSOC suggests that Part 6.4 could potentially be combined with 6.3, and perhaps even 6.5, for enhanced clarity.

Likes 0	
Dislikes 0	

Response

Alain Mukama - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

Although R6.4 allows the latitude for various INSM Methodologies and technologies; it also must satisfy R6.1. Hence, R6.1 should be defined in more detail. See response to Q4 above.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
There doesn’t appear to be much latitude in how to implement methodology.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
We support the comments as provided by EEI.	
Likes 0	
Dislikes 0	
Response	
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	
Answer	No
Document Name	

Comment

Tacoma Power does not agree that the Table R6 requirements allow latitude for various INSM methodologies. The NSM process described in R6 is one way to solve the Internal Network Security Monitoring Order, but other methodologies exist to gather and alert on malicious internal East/West traffic. It may be beneficial to recast the entirety of R6 in the Risk Mitigation ideal to mitigate the risk posed by malicious network activity within the CIP-Networked Environment.

Part 6.2 should include "per system capability" to ensure that entities are not required to collect data on systems that may not have the capability.

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	No
Document Name	

Comment

SPP does not agree the SDT was successful in creating an objective-based approach, particularly with the concerns expressed in SPP's comments for questions 4, 5, 6, 9, and 11.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Duke Energy greatly appreciates the work of the drafting team to create INSM requirements while trying to balance the need for flexible language. We are concerned that that the draft requirement allows too much latitude and will result in significant differences between INSM programs from responsible entity to responsible entity.

Likes 0	
Dislikes 0	

Response

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	
Based on the technical rational and the various diagrams that have been presented, SMUD believes that the INSM requirements are both prescriptive and subjective.	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Israel Perez On Behalf of: Mathew Weber, Salt River Project, 3, 1, 6, 5; Sarah Blankenship, Salt River Project, 3, 1, 6, 5; Thomas Johnson, Salt River Project, 3, 1, 6, 5; Timothy Singh, Salt River Project, 3, 1, 6, 5; - Israel Perez	
Answer	No
Document Name	
Comment	
A 'No' response is based on ambiguities but agree that latitude is allowed for various INSM methodologies and technologies to be used now and in the future.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	
PG&E believes some of the requirements need additional clarification, as noted in our earlier comments.	

Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
We are concerned that auditors may not agree with designations of BCSI over EACMS for the INSM system. The drafting team states in the technical rationale that BCSI is an acceptable designation. We feel that an INSM system meets the definition of an EACMS due to its electronic access monitoring capabilities, especially of non-encrypted protocols such as Telnet. In some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining "electronic access monitoring" as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
We do not find that R6 Part 1 is objective or will lead to objective outcomes. Please see comments above.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	

Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
Consider leveraging the OSI model to clearly identify the target depth of monitoring and retention. It is unclear what the level of information (eg Layer 2, 4, or 7) is required to be collected and stored to satisfy the requirement.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	

Comment	
We agree that Requirement R6, as written, provides latitude for various methodologies and technologies to be used. However, the broadness and ambiguity of some of the requirements and measures may lead to disagreements between entities and auditors that sufficient monitoring and documentation have been provided. Without providing more specific guidance on the type of information that should be available within data logs, retention periods, response timelines, and assessments of anomalous activities, this could lead to auditors issuing PNCs for an entity where they deem that the documentation being provided as evidence is insufficient.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Project 2023-03 SDT did create a requirement that was objective based and allowed latitude for various INSM methodologies, but this is a double-edged sword, with the large amount of latitude it leaves too much varying interpretations between what an auditor is expecting, and an entity is doing. In addition, there will be varying ways in which entities across different regions meet this requirement some will go above and beyond while others do the bare minimum which again leaves it up to an auditor if enough is being done to be compliant.	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	
Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees that the language in Requirement R6 is objective based and allows latitude for various entity INSM methodologies and technologies, noting our suggested changes proposed above.	
Likes 0	
Dislikes 0	
Response	

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer	Yes
Document Name	

Comment

We are concerned that auditors may not agree with designations of BCSI over EACMS for the INSM system. The drafting team states in the technical rationale that BCSI is an acceptable designation. We feel that an INSM system meets the definition of an EACMS due to its electronic access monitoring capabilities, especially of non-encrypted protocols such as Telnet. In some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.

Likes 0	
Dislikes 0	

Response

Selene Willis - Edison International - Southern California Edison Company - 5

Answer	Yes
Document Name	

Comment

“See comments submitted by the Edison Electric Institute”

Likes 0	
Dislikes 0	

Response

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

We are concerned that auditors may not agree with designations of BCSI over EACMS for the INSM system. The drafting team states in the technical rationale that BCSI is an acceptable designation. We feel that an INSM system meets the definition of an EACMS due to its electronic access monitoring capabilities, especially of non-encrypted protocols such as Telnet. In some cases where there are logging limitations on certain devices who

use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF believes that the proposed Requirement R6 is objective based and will allow for various INSM methodologies and technologies.	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	Yes
Document Name	

Comment	
This effort and work to meet the requirements and allow flexibility in execution of the requirements is greatly appreciated.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: “ EEI agrees that the language in Requirement R6 is objective based and allows latitude for various entity INSM methodologies and technologies, noting our suggested changes proposed above.“	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	Yes

Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees the language in Requirement R6 is objective and allows latitude, noting our proposed changes above.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
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 appreciates the efforts made by the SDT to make Requirement R6 objective based and to allow flexibility in execution. The responses provided to the other questions in this comment form are meant to clarify and reinforce this intent.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
MRO NSRF appreciates the efforts made by the SDT to make Requirement R6 objective based and to allow flexibility in execution. The responses provided to the other questions in this comment form are meant to clarify and reinforce this intent.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
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	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	

9. Do you agree with the Implementation Plan for Draft 1 of proposed CIP-007-X of 36 months for applicable systems located at Control Centers and backup Control Centers and 60 months for applicable systems not located at Control Centers? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The ambiguity with the proposed language makes it difficult to assess implementation timeframes.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
MRO NSRF appreciates the consideration given in this staggered implementation. There is no issue with the implementation plan itself in isolation. 36 months may or may not be sufficient depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient. The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	No

Document Name	
Comment	
With the increased concern of critical infrastructure infiltration by foreign adversaries, 36 months should be applied to all systems inside and outside of Control Centers. This should be conceivable since Part 6.1 provides latitude to not having 100% coverage of network data collection locations.	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
36 months for Control Centers and 60 months for applicable systems located outside Control Centers should be sufficient only if the language in Part 6.1 of “100 percent coverage is not required” is updated with the following (or similar): “*Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications based on the network risk as determined and documented by the Responsible Entity and per Cyber Asset or BES Cyber System capability or where technically feasible. Collection methods should provide security value to address the perceived risks.”*	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	

Comment

Without clear expectations of the Drafting Team toward the Industry Members, we cannot support the implementation Plan of CIP-007-x.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

In March 2022, BPA made the following comment in response to FERC's INSM NOPR:

"Bonneville estimates implementation timelines for INSM on High Impact BES Cyber Systems alone to be around three to five years. If entities are also required to adopt INSM on Medium Impact BES Cyber Systems with ERC, it would likely take on the longer end of that timeline to implement.

After reviewing the new requirement language in R6, BPA believes more time will be required to implement an INSM program. This takes into consideration the effort needed to create new processes and plans for INSM, procure new equipment (availability of vendors, products, and potential supply chain issues), modify networks, gather network information, and implement capabilities to consume network information and perform the necessary analysis. With that said, BPA recommends the SDT revise the implementation plan to state '60 months for high impact cyber systems (located at Control Centers and backup Control Centers), with an additional 24 months for medium impact cyber systems with ERC.'

Likes 0	
Dislikes 0	

Response

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	No
Document Name	

Comment

Manitoba Hydro appreciates the consideration given in this staggered implementation. There is no issue with the implementation plan itself in isolation. The 36 month timeline may or may not be sufficient depending on the reading of 6.1 regarding "100 percent coverage is not required." Per response to

Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient. The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
Dominion Energy has concern over the 36 month implementation due to supply chain concerns. Dominion Energy requestis 48 months for Control Center and keep 60 months for the other applicable systems not located at Control Centers.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	

Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
In light of the SDT's decision to declare some CIP devices outside of ESPs in scope, NST lacks the information necessary to either agree or disagree with the proposed schedule.	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No
Document Name	
Comment	
Unknown if 36 months is sufficient for implementation - it depends on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient. Further, the Technical Rationale on pg. 4 should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
There could be cases where entities may not be able to procure, test, configure, and fully deploy an INSM solution within the stated months. A suggestion is to allow each entity to respond with an appropriate timeframe for implementation that is viable to it. The Regional Entity can be afforded oversight to their entities’ commitment.	

Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP does not agree with the Implementation Plan for Draft 1 of proposed CIP-007-X based on the concerns expressed in SPP's comments for questions 4, 5, 6, 9, and 11.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	

In the implementation plan there should be a consistent approach to counting the effective date for applicable systems. LCRA recommends using 36 months and 60 months as written above instead of using the 36 months from regulatory approval and 24 months after effective date of standard as written in the current draft implementation plan.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
If the FERC Order involves monitoring INSM data for High/Medium assets and communication to/from specific types of PACS/EACMS within the ESP, GSOC finds the provided timeframe sufficient. Nevertheless, due to the ongoing lack of clarity in the scope, it is challenging for us to provide comments, resulting in a "No" response to this question.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
In the implementation plan there should be a consistent approach to counting the effective date for applicable systems. LCRA recommends using 36 months and 60 months as written above instead of using the 36 months from regulatory approval and 24 months after effective date of standard as written in the current draft implementation plan.	
Likes 0	
Dislikes 0	
Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	

Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	No
Document Name	
Comment	
SIGE does not agree with the implementation plan because implementation in generation and substation facilities will be extremely time consuming. Implementation within a high or medium Control Center will also be time consuming in order to ensure communications is not interrupted or adversely affected. Entities will also have to consider the fact that during this implementation period, there will most likely be system upgrades/replacements that have to be completed concurrent with the implementation of these new requirements. SIGE suggests revising the time period to 48 months for applicable systems located at Control Centers and backup Control Centers and 72 months for applicable systems not located at Control Centers.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
We appreciate the consideration given in this staggered implementation. There is no issue with the implementation plan itself in isolation. 36 months may or may not be sufficient depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs, 36 months should be sufficient. The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity	

to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by the MRO group.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	Yes
Document Name	
Comment	
PG&E agrees with the implementation plan.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	Yes
Document Name	
Comment	

Black Hills Corporation supports the proposed Implementation Plan, but 36 months would be the minimum time required to implement. Black Hills Corporation also agrees with the proposed changes from EEI, "EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

(remove "Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.")

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging."

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 6

Answer	Yes
Document Name	

Comment

Constellation has no additional comments.

Kimberly Turco on behalf on Constellation segements 5 and 6

Likes 0	
Dislikes 0	

Response

Byron Booker - Oncor Electric Delivery - 1

Answer	Yes
Document Name	

Comment

Oncor stands in agreement with comments presented by EEI that states:

"EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below). **Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.** Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging."	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the proposed Implementation Plan and the phased approach.	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	Yes
Document Name	
Comment	
NEE supports EEI comments: " EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below). **Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern**	

equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents. Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging. "	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes

Document Name	
Comment	
The NAGF supports the proposed implementation plan.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	Yes
Document Name	
Comment	
“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	Yes
Document Name	
Comment	
The implementation plan could clarify these timelines better and how they stack. Currently it is not obvious.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	

Comment

Avista agrees with EEI's comments and recommendation for Technical Rationale:

EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

Remove the following:

Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment

capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.

Insert the Following:

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI supports the proposed Implementation Plan, however, we are concerned with the statement in the Technical Rationale (see page 4 under the Section titled Vendor Support), noting that the industry needs the flexibility to balance system upgrades with the known risks. To address this concern, we offer the following edits to the Technical Rationale, Page 4, Vendor Support (Changes in boldface below).

Instances where legacy control systems do not have the capability to support INSM or endpoint logging, consideration should be given to updating the legacy system, or finding other solutions that might provide an equivalent method of security monitoring and logging.

Likes 0	
Dislikes 0	

Response

Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	Yes
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	Yes
Document Name	
Comment	
Avista agrees with EEI’s comments and recommendation for Technical Rationale:	
Likes 0	
Dislikes 0	
Response	
Robert Blackney - Edison International - Southern California Edison Company - 1	

Answer	Yes
Document Name	
Comment	
See comments submitted by the Edison Electric Institute.	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
3 years for Control Centers and 5 years for non-control centers is acceptable but more technical guidance or requirement clarity is required to meet auditors' expectations. The technical rational and guidance need more clarity to align the auditors and implementors.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Yes, however the more time the better some entities will already have upgrades planned and this will have to be figured into the upgrades.	
Likes 0	
Dislikes 0	
Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	
Southern Company agrees with the implementation duration. However, Southern Company would offer the suggestion to have separate sentences with "…the standard shall become effective for Control Centers on the first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees". "…the standard shall become effective for medium impact BES Cyber Systems with ERC not located at Control Centers on the first day of the first calendar quarter that is sixty (60) months after the date the standard is adopted by the NERC Board of Trustees". We believe this would help with confusion that is occurring with the Implementation Plan as currently written.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	Yes
Document Name	
Comment	
Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

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	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
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	
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	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Joshua London - Eversource Energy - 1, Group Name Eversource	
Answer	
Document Name	
Comment	
Eversource supports the comments of EEI.	
Likes 0	
Dislikes 0	
Response	

10. Do you agree that the modifications made in Draft 1 or proposed CIP-007-X are cost effective? If you do not agree, please provide your recommendation, and if appropriate, technical or procedural justification.	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	No
Document Name	
Comment	
Developing and maintaining the necessary processes and procedures to maintain a sufficient level of documentation for compliance purposes will create a need for entities to increase the number of FTEs. We have already seen an increase in costs associated with INSM from vendors over that past few years and expect that once this requirement is approved, costs will increase further due to the limited number of vendors with applicable OT solutions.	
Likes 0	
Dislikes 0	
Response	
Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
May or may not be cost effective depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs costs could be contained to a reasonable amount. The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Jennifer Buckman - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	

Answer	No
Document Name	
Comment	
No, without further study, SIGE believes the costs associated with the new requirements cannot be determined. Some generation and substation facilities will require equipment replacement in order to meet these requirements. It will take an untold number of man-hours to evaluate and identify collection locations and methods to collect data. Entities will most likely have to add additional personnel in order to maintain compliance with the ongoing requirements to review the data collected for anomalous activity.	
Likes 0	
Dislikes 0	
Response	
Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company	
Answer	No
Document Name	
Comment	
It is Southern Company's opinion that the cost effectiveness of the current proposed requirements can vary greatly depending on what percentage below 100% in R6.1 is determined to be compliant in each region, and what specific Cyber Assets are determined to require monitoring. In addition, there are significant concerns about supply chain constraints given a limited pool of Operational Technology (OT) vendors with INSM products.	
Likes 0	
Dislikes 0	
Response	
Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Cost effectiveness is difficult to judge with the first draft. Ultimately cost effectiveness will be determined by the final draft. Additional oversite and help may be required for compliance.	
Likes 0	
Dislikes 0	

Response	
Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	
WEC Energy Group supports MRO's NERC Standards Review Forum's (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
High-cost tools and technology will be required. There will likely be a need for additional Subject Matter Experts (SMEs) to manage new tools and respond to alerting.	
Likes 0	
Dislikes 0	
Response	
Katrina Lyons - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
If the scope of the FERC Order requires monitoring INSM data for High/Medium assets and communication to/from specific types of PACS/EACMS within the ESP, GSOC contends that cost-effective solutions can achieve this goal. However, there is ambiguity in interpreting how to manage EACMS and PACS INSM data. In instances where these Cyber Assets might exist outside the ESP, it becomes unclear how much equipment would be necessary to retrofit existing infrastructures.	
Likes 0	

Dislikes 0	
Response	
James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin	
Answer	No
Document Name	
Comment	
High-cost tools and technology will be required. There will likely be a need for additional Subject Matter Experts (SMEs) to manage new tools and respond to alerting.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
The new requirement is inherently not cost effective.	
Likes 0	

Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	No
Document Name	
Comment	
Dependent on product purchased, staff augmentation, and size of utility, the impact of the cost to implement INSM would vary greatly.	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	No
Document Name	
Comment	
The cost to implement this requirement will be significant, not enough information at this time to determine cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Whitney Wallace - Calpine Corporation - 5	
Answer	No
Document Name	
Comment	
The implementation of this will cost money and significant resources to whomever implements it; however, there appears to be enough flexibility that companies can determine the robustness and strength of their program based on limited budget. To do it right, it will be expensive and require resources.	
Likes 0	

Dislikes 0	
Response	
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	
Answer	No
Document Name	
Comment	
Tacoma Power needs additional clarity to understand the scope of work and boundaries of what's covered in this Standard in order to assess cost.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
GO/GOPs will need more information to adequately assess the cost effectiveness of the proposed approach.	
Likes 0	
Dislikes 0	
Response	
David Bueche - Calpine Corporation - NA - Not Applicable - WECC,Texas RE,NPCC,SERC,RF	
Answer	No
Document Name	
Comment	
The implementation of this will cost money and significant resources to whomever implements it; however, there appears to be enough flexibility that companies can determine the robustness and strength of their program based on limited budget. To do it right, it will be expensive and require resources.	

Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No
Document Name	
Comment	
SPP asks the SDT to consider the potential cost that may arise from the scope of this requirement. As noted in other supporting documents related to INSM, the costs associated with capturing, analyzing, and storing of all data between every cyber assets within an ESP, for any length of time, will be substantial. Not all network architectures are created equal and could be more costly and time consuming to implement for some Responsible Entities than others. Virtualization of network, server, and storage infrastructure, and the complexity it brings to the table, has the potentiality to make packet captures, baselining of traffic, monitoring, analyzing, and alerting much more difficult if a Responsible Entity is unable to obtain visibility into all of the network traffic within a subnet.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
It is not clear that all sub parts of requirement R6 could be cost effective. It is a new requirement that would mandate an entity to effectively not only procure a brand new solution, but produce an entirely new process and procedures, in addition to the human resources and associated roles and responsibilities, with which the entity must comply. Although it’s possible certain entities would not have a financial burden for this kind of expenditure, it may be a significant burden for others.	
Likes 0	
Dislikes 0	
Response	
Jennifer Neville - Western Area Power Administration - 6	
Answer	No

Document Name	
Comment	
The cost effectiveness is dependent upon updating the langauge to 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs costs could be contained to a reasonable amount. Further, the Technical Rationale on pg. 4 should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware would take longer if required and may not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Roger Fradenburgh On Behalf of: Nick Lauriat, Network and Security Technologies, 1; - Roger Fradenburgh	
Answer	No
Document Name	
Comment	
In light of the SDT's decision to declare some CIP devices outside of ESPs in scope, NST lacks the information necessary to either agree or disagree the proposed changes are cost-effective.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
This inclusion of cyber assets outside of High BCS and Medium BCS with ERC is not the most cost-effective approach to increasing the security posture of those cyber assets. Addressing boundary-level (north-south) controls for these assets would be more cost-effective approach and a logical first step to creating a common understanding of a “trust zone” for these device types before an east-west monitoring construct is applied.	
Likes 0	
Dislikes 0	
Response	
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 feels that the determination of cost effectiveness varies based on the methodology used, but prescribing network communication baselines as the methodology would not be cost effective.	
Likes 0	
Dislikes 0	
Response	
Alison Nickells - NiSource - Northern Indiana Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
NIPSCO has not determined whether R6 will be cost effective. The procurement process for a tool(s) and resources will be initiated should the requirement language remain as is.	

Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	No
Document Name	
Comment	
The expansion of the scope of the FERC Order to include PCA, EACMS, and PACS will significantly increase the implementation costs. Although the standards drafting team indicated that assets not currently in scope of the CIP standards are not included (for example, Corporate AD servers that are not currently EACMS), it is likely that audit teams will have different interpretations.	
Likes 0	
Dislikes 0	
Response	
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	
Not too sure what the exact cost will be for each entity, but the cost of monitoring can be a costly endeavor for many entities, including SRP.	
Likes 0	
Dislikes 0	
Response	
Michael Johnson - Michael Johnson On Behalf of: Frank Lee, Pacific Gas and Electric Company, 3, 1, 5; Marco Rios, Pacific Gas and Electric Company, 3, 1, 5; Sandra Ellis, Pacific Gas and Electric Company, 3, 1, 5; - Michael Johnson, Group Name PG&E All Segments	
Answer	No
Document Name	
Comment	

PG&E cannot determine if the modifications are cost effective at this time.   There are still unknowns as to the required scope (% coverage) and data retention requirements. We would like to see more industry feedback before deciding.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

AECI supports comments provided by the MRO group.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer	No
Document Name	

Comment

May or may not be cost effective depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs costs could be contained to a reasonable amount.

The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware may not be cost effective.

Likes 0	
Dislikes 0	

Response

Jeffrey Streifling - NB Power Corporation - 1	
Answer	No
Document Name	
Comment	
There are significant costs involved in standing up and monitoring an INSM. While the cyber security benefits are obvious to IT professionals, they are not as clear to executives. Many entities are unable to hire staff and invest in technology freely due to cost restriction initiatives.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 4, Group Name FE Voter	
Answer	No
Document Name	
Comment	
This change in the standard will result in significant resource expenditure, including wholesale replacement/architecture of existing networks, that will be exceptionally costly and such costs will be passed on. Implementing this standard will result in the potential of hundreds of network devices all requiring replacement with devices that are significantly more costly simply to add the ability to execute some form of intra-lan monitoring. Additionally, the potential reliability impact of requiring major network architecture needed is much higher than modest security gains.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	No
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	

Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	No
Document Name	
Comment	
Depending on if the language in Part 6.1 is updated, this may or may not be cost effective. If the language of “100 percent coverage is not required” is updated with language similar to the following: “*Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications based on the network risk as determined and documented by the Responsible Entity and per Cyber Asset or BES Cyber System capability or where technically feasible. Collection methods should provide security value to address the perceived risks.”*, then the implementation plan should be sufficient as proposed by the SDT.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	No
Document Name	
Comment	
May or may not be cost effective depending on the reading of 6.1 regarding “100 percent coverage is not required.” Per response to Q4 this should be removed and replaced by continuing the first sentence with “commensurate with network risk as determined by the Responsible Entity.” If Part 6.1 governs costs could be contained to a reasonable amount. The problem is with the Technical Rationale regarding Vendor Support on p. 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” This is inconsistent with the webinar statements that work-arounds are almost always possible. The Technical Rationale should be modified to replace “may need to” with “could” and should add alternative options regarding monitoring workarounds. Retrofitting “outdated” hardware may not be cost effective.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name TVA RBB	
Answer	No
Document Name	
Comment	
The ambiguity with the proposed language makes it difficult to assess implementation cost.	
Likes 0	
Dislikes 0	
Response	
Clay Walker - Cleco Corporation - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alain Mukama - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Agree and disagree. Since the standard allows the latitude, cost effective solutions can be implemented but will it be good enough to meet the auditor's expectations? The technical rational and guidance need more clarity to align auditors and implementors.	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Quebec (HQ) - 1	

Answer	Yes
Document Name	
Comment	
There are significant costs involved in standing up and monitoring an INSM. While the cyber security benefits are obvious to IT professionals, they are not as clear to executives. Many entities are unable to hire staff and invest in technology freely due to cost restriction initiatives	
Likes 0	
Dislikes 0	
Response	
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	
There are significant costs involved in standing up and monitoring an INSM. While the cyber security benefits are obvious to IT professionals, they are not as clear to executives. Many entities are unable to hire staff and invest in technology freely due to cost restriction initiatives.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Kimberly Turco - Constellation - 6	
Answer	Yes
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon Smith - Brandon Smith On Behalf of: Marcus Bortman, APS - Arizona Public Service Co., 1, 3, 6, 5; - Brandon Smith	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Lindsey Mannion - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anne Kronshage - Anne Kronshage, Group Name Public Utility District No. 1 of Chelan County - Voting Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	
Document Name	

Comment	
The cost to implement this requirement will be significant, not enough information at this time to determine cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Marcus Sabo - Marcus Sabo On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Marcus Sabo	
Answer	
Document Name	
Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 3	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Selene Willis - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	

“See comments submitted by the Edison Electric Institute”	
Likes 0	
Dislikes 0	
Response	
Bobbi Welch - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	
MISO supports the comments submitted by the ISO/RTO Council Standards Review Committee (SRC).	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE does not comment on cost effectiveness.	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	

NA	
Likes 0	
Dislikes 0	
Response	
Byron Booker - Oncor Electric Delivery - 1	
Answer	
Document Name	
Comment	
Oncor will not submit comments on the cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 6, Group Name Proj 2023-03 INSM	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost effectiveness of the proposed changes.	
Likes 0	
Dislikes 0	
Response	
Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	

BPA cannot determine cost effectiveness at this point. It is difficult to make such a determination when new/revised requirements may constitute the acquisition of new technology, equipment, and staff training.	
Likes 0	
Dislikes 0	
Response	

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

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

Answer	
Document Name	

Comment

Data retention requirements are ambiguous and subject to interpretation by entities and the CEA. Suggest revise to provide guidance regarding retention requirements by data type.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

MRO NSRF appreciates the approach the SDT took in drafting this standard revision to focus on outcomes without undue proscription or limitations in execution. We hope these offered refinements and considerations will help speed us to an affirmative ballot.

For Part 6.1 we wonder if there is any intentional overlap regarding CIP-012 communications between control centers. Internal network security monitoring between applicable Cyber Assets would seem to preclude communications between control centers. Will the SDT please explain if CIP-012 communications are included under the 6.1 phrase "network communications between applicable Cyber Assets," or does this language exclude CIP-012 communications? Could we add the qualifying word "internal" between "Identify" and "network?"

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add "from Part 6.2" after "data collected" in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add "as determined by the documented processes or procedures of the Responsible Entity."

Please replace the Measure for Part 6.2 with the language from the Technical Rationale: "When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to: Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic; Forwarding log information to a searchable database for retention; or Summarizing logs in a searchable database.

Part 6.7 uses the term “adversary.” We feel this is a loaded term that is not needed. Deleting “by an adversary” would not diminish data protection. Regarding CIP-008, MRO NSRF urges the drafting team to include requirement language making it clear that at some point, if investigation of anomalous activity indicates an actual attack or attempt to compromise, that CIP-007 R6 ends and CIP-008 requirements take over. We understand that that is the intent of the drafting team – that CIP-007 R6 could lead into CIP-008 – but the requirement language so far does not indicate that clearly and instead allows for potential of overlap in compliance obligations. The proposed requirement language needs to be clarified to address this point. Lastly, MRO NSRF thanks the SDT for their industry outreach, and hopes we can continue such collaboration as this draft is revised to hopefully reduce ballot iteration and come more quickly to consensus.	
Likes 0	
Dislikes 0	
Response	
Karen Artola - CPS Energy - 1,3,5 - Texas RE	
Answer	
Document Name	
Comment	
For Part 6.5, reword sentence to begin, “Develop one or more process(es)…” For Part 6.7, reword sentence to begin, “Develop one or more process(es)…”	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - Rebika Yitna On Behalf of: Roger Brand, MEAG Power, 3, 1; - Rebika Yitna	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
OPG supports NPCC Regional Standards Committee’s comments.	
Likes 0	
Dislikes 0	
Response	
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	
None.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	

Answer	
Document Name	

Comment

We feel that an INSM system meets the definition of an EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

If the INSM system can detect and alert on events such as brute force attacks, even if inferred, this still constitutes electronic access monitoring of a BES Cyber System in our opinion. If our interpretation is incorrect, then the term EACMS must be altered to define more clearly “electronic access monitoring”, or some very specific verbiage be provided in the standard itself as to why the INSM does not meet the definition of EACMS. If logs directly from a device are required for a devices to be categorized as EACMS, then that must be stated explicitly in the definition.

As stated in the Comments for Question 8 above, in some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.

INSM is basically about collection and analysis of network communications within CIP networked environment. This is all about monitoring and the systems used for this purpose should be classified as EACMS being Electronic Monitoring system. This is an extension of log monitoring systems which are classified as EACMS.

The idea of not classifying INSM systems by proposing that BCSI or EACMS protection be utilized may lead to avoidable confusion down the line.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

BPA recommends adding language addressing the intended periodicity or ongoing nature of the proposed R6 Parts. BPA can’t determine based on the proposed requirement language how often the ERO-Enterprise (ERO-E) would expect entities to perform the location identification, data logging, and baselining requirements. In order to avoid inconsistent interpretations among Registered Entities and auditors across the ERO-E, BPA recommends the SDT include language in the requirements that specifies a minimum cadence by which the aforementioned tasks should be completed or that clarifies the RE is empowered to determine the cadence. The SDT should clarify if the intent is to have methods and processes for R6.4 through R6.6 that address patterns of behavior and processes to analyze them, rather than isolated pieces of traffic.

BPA also recommends adding minimum log retention timeframes as a compliance metric and to align with other CIP standards. R6.7 should be modified to cover risk of data exploitation as follows: “…protect the data collected in Part 6.2 to mitigate the risks of exploitation, deletion, or modification by an adversary…”

Likes 0

Dislikes 0

Response

Jay Sethi - Jay Sethi On Behalf of: Nazra Gladu, Manitoba Hydro , 1, 3, 5, 6; - Jay Sethi, Group Name Manitoba Hydro Group

Answer

Document Name

Comment

Manitoba Hydro appreciates the approach the SDT took in drafting this standard revision to focus on outcomes without undue proscription or limitations in execution. We hope these offered refinements and considerations will help speed us to an affirmative ballot.

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add “as determined by the documented processes or procedures of the Responsible Entity.”

Please replace the Measure for Part 6.2 with the language from the Technical Rationale: “When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to: Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic; Forwarding log information to a searchable database for retention; or Summarizing logs in a searchable database.

Part 6.7 uses the term “adversary.” We feel this is a loaded term that is not needed. Deleting “by an adversary” would not diminish data protection.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

AECI supports comments provided by the MRO group.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

PG&E appreciates the effort the DT had taken in creating a Standard to meet FERCs Order with a very aggressive time frame. PG&E will be waiting to see the next version of these requirements based on our and other Registered Entities feedback that include the scope and percentage of coverage of Cyber Assets**.**

Likes 0

Dislikes 0

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer

Document Name

Comment

Section 4 comment: The standard should clearly indicate that the entity would be responsible for performing an assessment (preferably risk based) from which the most critical interfaces (chosen by the entity) will be applicable to 6.1. The entity should also consider documenting the reasons why others were not considered critical.

Stating "100 percent coverage is not required" can lead the entities to only monitor a few CIP network interfaces without any clear direction to comply with the standard, and not use this opportunity for the intent purpose of the standard to monitor and protect the internal networks from security threats.

Section 6 comment: Per the information gathered from CIP-007-X, the use of word “anomalous” doesn’t clearly indicate the use of both network baseline and the signature-based tools to identify anomalous. E.g., 6.4 states “Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2” which could lead entities to use only log collected data and not network baselines indicated in 6.3 to detect anomalous (including malicious) activities.

Additionally, SDT should consider defining anomalous to avoid any confusion for entities.

Additional Comment

There is no requirement to reevaluate the environment after changes or on a periodic basis to ensure that the entity is monitoring the higher risk traffic.

Likes 0

Dislikes 0	
Response	
Kimberly Turco - Constellation - 6	
Answer	
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf on Constellation segements 5 and 6	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
It appears by the name of the R6 table, Internal Network Security Monitoring, the intent of this requirement is to monitor internal network traffic. However, this intent is not present in the requirement language. For example, Requirement R6 Part 6.1 states that communications between applicable Cyber Assets are in scope. High impact BCS are in scope, as are medium impact BCS with External Routable Connectivity. These BCS are commonly found in discrete networks, however the requirement language does not clearly exclude from scope communications between these applicable systems found in discrete networks. If the SDT intends for communications between Applicable Systems in discrete networks to be in scope, then no change is needed. If the SDT does not intend for communications between Applicable Systems in discrete networks to be in scope, Texas RE recommends modifying the requirement language to convey this.	
Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Byron Booker - Oncor Electric Delivery - 1

Answer	
Document Name	

Comment

Oncor stands in agreement withg the comments being submitted by EEI that states:

"BCSI Implications (NEW Proposed)

For entities that do not have an internal security monitoring center and may desire to use a cloud-based service, or even onsite monitoring tools today that may have cloud-based data analysis components, there needs to be clarity on the BCSI implications of the data. Page 3 of the Technical Rationale states “Ideally, the NSM system would only be designated as BCSI”, which brings into question the impacts of CIP-004 for cloud vendor personnel where a security monitoring service may require provisioned access to “obtain and use” the BCSI in order to perform the security monitoring function and alert the entity to any anomalies it sees in the data received.

(NEW Proposed) EEI is concerned that in Requirement R6, the phrase “that has bypassed other security controls” is too broad and generic of an objective statement as there are attacks that may bypass “security controls”, such as CIP-006 physical security controls, that INSM will not detect. Suggest either deleting this phrase or changing it to “detecting attacks that may bypass electronic security perimeters”.

EEI suggested adding “in Part 6.4” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.2** with sufficient detail and duration to support the investigation of anomalous activity.

(**NEW Proposed**) EEI additionally suggests the following boldface edits (below) for Requirement 6, part 6.5 to make it clearer the expectation that entities have when they are evaluating anomalous activity.

6.5 One or more process(es) to evaluate anomalous activity identified in Part 6.4 **and to determine appropriate action which include a process for:** **6.5.1: Identifying an attack in progress and actions to be taken in response; and** **6.5.2 Evaluating anomalous activities and actions to be taken in response."**	
Likes 0	
Dislikes 0	
Response	
Donna Wood - Tri-State G and T Association, Inc. - 1	
Answer	
Document Name	
Comment	
NA	
Likes 0	
Dislikes 0	
Response	
Jeffrey Icke - Colorado Springs Utilities - 5	
Answer	
Document Name	
Comment	
If the scope of this proposed standard was limited to the scope of the FERC Order (assets within the Electronic Security Perimeter), then this standard language should be part of CIP-005, not CIP-007.	
Likes 0	
Dislikes 0	
Response	
Mark Flanary - Midwest Reliability Organization - 10	
Answer	

Document Name

Comment

1. Part 6.5 language is inconsistent with the other R6 sub-parts. All others start with an action verb. We suggest updating 6.5 to begin as "Evaluate anomalous activity...". The process language is inherited from the higher-level R6 requirement language.

2. Part 6.7 - Same statement as for Part 6.5 - We suggest beginning it with "Protect the data collected..."

Likes 0

Dislikes 0

Response

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

Document Name

Comment

SMUD appreciates the Standard Drafting Team’s effort to revise CIP-007-X to include INSM requirements, but we have the following additional recommendations:

- Move Requirement R6 Part 6.4 (deploy) so that it is before Part 6.2 (log). Part 6.4 should become Part 6.2, then Part 6.2 will then become 6.3, and Part 6.3 will become Part 6.4 with all other parts staying where they are;

- Move all INSM requirements and parts to CIP-005; and

- In the Applicable Systems column, just state EACMS and/or PACS. Do not add where they perform access control functions. There are no other CIP requirements that state anything other than EACMS and/or PACS.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

Duke Energy thanks the Drafting Team for their work to thoughtfully address FERC Order 887. There are some additional items that we would like to recommend to add clarity to the INSM revisions.

- Duke Energy recommends Requirement 6.1 is updated to require entities to specify the types of data to be collected in their documented processes, so that the data that will be expected for part 6.2 is clearly tied back to part 6.1.
- Additionally, use of the same phrase “network data” in 6.1 and 6.2 would bring greater clarity to the requirements, updating 6.2 to read “Log collected network data at the network locations identified in Part 6.1.”
- We also request clarity on the use of the term “connections” in 6.1. Does this intend to refer to TCP/UDP “connections” or the connecting and disconnecting of devices to network switches or some other definition of this term? Alternative language such as “monitor and detect anomalous activity, including the presence of anomalous devices in the network and use of anomalous communication protocols in the network” would provide a clearer requirement.
- Duke Energy also recommends that the INSM requirements are moved to their own Standard outside of CIP-007. CIP-007’s traditional focus on device-level security controls is at odds with the broader subject matter of network monitoring, and following the model used by CIP-012 for a new subject matter with no current analogous scoping would facilitate the introduction of this technology and scope, as well as lay the groundwork for elimination of duplicate requirement language in CIP-007 and CIP-003 if Low applicability later added.

Likes 0	
Dislikes 0	

Response

Joshua London - Eversource Energy - 1, Group Name Eversource

Answer	
Document Name	

Comment

For Part 6.1 we wonder if there is any intentional overlap regarding CIP-012 communications between control centers. Internal network security monitoring between applicable Cyber Assets would seem to preclude communications between control centers. Will the SDT please explain if CIP-012 communications are included under the 6.1 phrase “network communications between applicable Cyber Assets,” or does this language exclude CIP-012 communications? Could we add the qualifying word “internal” between “Identify” and “network?”

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add “as determined by the documented processes or procedures of the Responsible Entity.”

Similar to above, suggested adding “in Part 6.4” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.4** with sufficient detail and duration to support the investigation of anomalous activity.

Likes 0

Dislikes 0

Response

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

Answer

Document Name

Comment

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

Likes 0

Dislikes 0

Response

Richard Vendetti - NextEra Energy - 5

Answer

Document Name

Comment

NEE agrees with two of EEI additional comments:

“EEI is concerned that in Requirement R6, the phrase “that has bypassed other security controls” is too broad and generic of an objective statement as there are attacks that may bypass “security controls”, such as CIP-006 physical security controls, that INSM will not detect. To address this concern, we suggest either deleting this phrase or changing it to “that has bypassed other electronic security controls”.

EEI suggested adding “in Part 6.2” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.2** with sufficient detail and duration to support the investigation of anomalous activity. “

“Data Collection Methods, Pages 9 through 10

The term “CIP-networked environment” is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document, section "Data Collection Methods," on pages 9 through 10, outlines considerations for data collection which include Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. To address this concern, we suggest that revisions be made to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.”	
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 believes it would be helpful for R6 Part 6.6 to identify a minimum retention period for INSM data unless the SDT intends for it to be the standard 3-year period defined in Section C Part 1.2 ("Evidence Retention"). The language in the proposed Measure for 6.6, "...with data retention configuration with timelines sufficient to perform the analysis of anomalous activity" is vague and could easily be subject to a considerable number of widely different interpretations.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5	
Answer	
Document Name	
Comment	
Constellation has no additional comments Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

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

Answer

Document Name

Comment

In Part 6.2, the measure describes an example evidence, which is the data collected. It is not clear why the focus is on the data collected and not the configuration of logging the data, which is the actual stated requirement.

Observation: CIP-007 R6 applicability assumes all assets are known and classified according to CIP-002 and only requires baselining of network traffic between applicable assets. But if an unknown malicious device is put on the network, because it is unclassified and not a BCA, PCA, EACMS, or PACS, and is on its own interface, the entity does not have to pay attention to it or its anomalies. Example – if someone installs a rogue device on the network that initiates a portscan, the entity does not have to recognize the device or the portscan as a network baseline deviation. Along those lines, because TCAs are excluded from applicability, the entity does not have to pay attention to TCAs even though their insertion on the network at odd hours may be anomalous. The structure allows the entity to entirely ignore rogue devices as an attack vector.

Likes 0

Dislikes 0

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer

Document Name

Comment

SPP would like the SDT to consider the following:

Comment for Part 6.2:

SPP is concerned with the requirement language for Part 6.2. The proposed language is open to interpretation and could significantly impact the cost of storage as well as create compliance risk. What needs to be logged? How should the log be evidenced? Is a summary sufficient? How long do the logs need to be retained?

Comment for Part 6.4:

The proposed language for Part 6.4 is too prescriptive, which conflicts with the language in FERC Order 887 asking for an objective-based approach.

SPP proposes the following language for Part 6.4:

Using the data collected pursuant to Part 6.2, deploy one or more method(s) to detect anomalous network activity indicative of an attack in progress.

Comment for Part 6.5:

SPP suggests replacing the word “process” with the word “method” to allow more flexibility with implementing this requirement.

SPP proposes the following language for Part 6.4:

One or more method(s) to evaluate the anomalous network activity indicative of an attack in progress identified in Part 6.4 and determine appropriate action.

Comment for Part 6.6:

The proposed language for Part 6.6 is too prescriptive, which conflicts with the language in FERC Order 887 asking for an objective-based approach.

SPP proposes the following language for Part 6.6:

One or more method(s) to investigate anomalous network activity indicative of an attack in progress.

Comment for Part 6.7:

SPP does not agree with using the term “adversary” in a NERC requirement due to its ambiguity. SPP also suggests replacing the word “process” with the word “method” to allow more flexibility with implementing this requirement.

Likes 0

Dislikes 0

Response

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

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

Answer

Document Name

Comment

TPWR believes that the INSM Requirements fit better in CIP-005, due to the Purpose statement found in the latest CIP-005-8: "To protect BES Cyber Systems (BCS) against compromise by permitting only known and controlled communication to reduce the likelihood of misoperation or instability in the Bulk Electric System (BES).", **than in CIP-007 which contains the Purpose** "To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)." The Title of CIP-005 may be due for an update as well, since the Title remains "Electronic Security Perimeter(s)" which is no longer fully inclusive of all that CIP-005 includes. One option for the Title of CIP-005 would simply be "Network Security."

Tacoma Power offers this language for the high level R6:

"Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-XXX-X Table RX – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed network perimeter-based security controls."

Tacoma Power believes that the requirement language provided does not align with the scope of monitoring identified in the Webinar on the slide titled 'Interpretation of the Term "CIP Networked Environment"'. Specifically, many of the red "out-of-scope" network paths are not out of scope based on the requirement language. Specifically between the EACMS/EAP and the EACMS Access Control and the EACSM/Intermediate System. EACMS/EAPs and EACMS/IS both perform access control functions and are therefore specifically included in scope. Additionally there are a significant number of additional "in-scope" network paths that are not clarified on the diagram, since the diagram only includes a single ESP and the current language does not limit the scope to the networks associated to each individual Applicable System.

Editorial Comments on Section 3, Purpose:

- The purpose statement should include the acronym after "BES Cyber Systems", as follows:

"To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems **(BCS)** against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)."

Editorial Comments on Section 4, Applicability:

- The term "Special Protection System" and "SPS" should be deleted throughout Section 4.
- Regarding Bullet 4.2.3.5: delete "-5.1" from CIP-002-5.1. The bullet should read "Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the **CIP-002** identification and categorization processes."
- The following exemption is missing and should be added as Bullet 4.2.3.3: "4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations."
- Bullet 4.3 is missing. Recommend adding this bullet, as follows: "4.3. "Applicable Systems": Each table has an "Applicable Systems" column to define the scope of systems to which a specific requirement part applies."
- Bullets 4.2.3.1 and 4.2.3.2 should refer to "Cyber Systems" and not "Cyber Assets"

Editorial comments on Table R6:

- In the "Applicable Systems" column, the word "impact" should not be capitalized. Additionally, the acronym "BCS" should be used instead of "BES Cyber System" and "ERC" instead of "External Routable Connectivity." Example of how this should be written: "Medium **impact** **BCS** with **ERC** and their associated…"

Comments related to alignment with Project 2016-02, CIP Virtualization:

- The title of CIP-007 Table R1 should be changed from "Ports and Services" to "System Hardening" to align with the Project 2016-02 changes. The title of Table R1 should also be changed in the R1 language.
- The title of CIP-007 Table R2 should be changed to "Cyber Security Patch Management" to align with Project 2016-02.

- The language in the following Requirement Tables in the CIP-007 redline do not match the changes in Project 2016-02. Tacoma Power recommends updating these tables to align with the recent CIP-007 draft in Project 2016-02.
- Table R1: Part 1.1 and Part 1.2 need to be updated. Part 1.3 is missing from Table R1.
- Table R2: Parts 2.1 through 2.4 need to be updated.
- Table R3: Parts 3.1 through 3.3 need to be updated.
- Table R4: Parts 4.1 through 4.4 need to be updated.
- Table R5: Parts 5.1 through 5.7 need to be updated.
- The Violation Severity Levels table should also be updated to align with the Project 2016-02 changes.
- Table R6, Parts 6.1 through 6.7 should include this statement at the end of the Applicable Systems list: “SCI supporting an Applicable System in this Part.”

Other Editorial Comments:

- “C. Regional Variances” should be “D. Regional Variances”
- The Section E, Interpretations, is missing. Recommend adding this section.
- “D. Associated Documents” should be “F. Associated Documents”.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

The SRC notes that Parts 6.5 and 6.7 use different phrasing than the remaining parts of Requirement R6, and recommends that Parts 6.5 and 6.7 be revised to begin with "Implement one or more process(es)..." to better align with the language used in the rest of Requirement R6.

Likes 0	
Dislikes 0	

Response

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

It is unclear how precise an anticipated network communication needs to be. How much of a deviation is anticipated / tolerated? In the proposed CIP-007 R6.1.

Consider the language in CIP-007 R4.1 as an example as how to identify any anomalous activity detection of security events noted in CIP-007 R4.

We feel that an INSM system meets the definition of an EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

If the INSM system can detect and alert on events such as brute force attacks, even if inferred, this still constitutes electronic access monitoring of a BES Cyber System in our opinion. If our interpretation is incorrect, then the term EACMS must be altered to define more clearly “electronic access monitoring”, or some very specific verbiage be provided in the standard itself as to why the INSM does not meet the definition of EACMS. If logs directly from a device are required for a devices to be categorized as EACMS, then that must be stated explicitly in the definition.

As stated in the Comments for Question 8 above, in some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining “electronic access monitoring” as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.

INSM is basically about collection and analysis of network communications within CIP networked environment. This is all about monitoring and the systems used for this purpose should be classified as EACMS being Electronic Monitoring system. This is an extension of log monitoring systems which are classified as EACMS.

The idea of not classifying INSM systems by proposing that BCSI or EACMS protection be utilized may lead to avoidable confusion down the line.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Quebec (HQ) - 1

Answer	
Document Name	

Comment

It is unclear how precise an anticipated network communication needs to be. How much of a deviation is anticipated / tolerated? In the proposed CIP-007 R6.1.

Consider the language in CIP-007 R4.1 as an example as how to identify any anomalous activity detection of security events noted in CIP-007 R4.

We feel that an INSM system meets the definition of an EACMS: “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems”.

If the INSM system can detect and alert on events such as brute force attacks, even if inferred, this still constitutes electronic access monitoring of a BES Cyber System in our opinion. If our interpretation is incorrect, then the term EACMS must be altered to define more clearly “electronic access monitoring", or some very specific verbiage be provided in the standard itself as to why the INSM does not meet the definition of EACMS. If logs directly from a device are required for a devices to be categorized as EACMS, then that must be stated explicitly in the definition.

As stated in the Comments for Question 8 above, in some cases where there are logging limitations on certain devices who use Telnet, the INSM could be the only method for monitoring electronic access to these devices and would be used to satisfy CIP-007 R4.1 at the BES Cyber System level. The INSM could also be used to meet the requirement in CIP-007-R5.7 for alerting after a threshold of unsuccessful authentication attempts. This would make the INSM EACMS as it would be the only device capable of monitoring electronic access to these types of devices. Without explicitly defining "electronic access monitoring" as it appears in the EACMS definition, we feel that any INSM meets the criteria to be categorized EACMS.

INSM is basically about collection and analysis of network communications within CIP networked environment. This is all about monitoring and the systems used for this purpose should be classified as EACMS being Electronic Monitoring system. This is an extension of log monitoring systems which are classified as EACMS.

The idea of not classifying INSM systems by proposing that BCSI or EACMS protection be utilized may lead to avoidable confusion down the line.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 3

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Glen Farmer - Avista - Avista Corporation - 5

Answer	
Document Name	

Comment

Avista agrees with EEI's comment:

EEI suggested adding "in Part 6.4" to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.4** with sufficient detail and duration to support the investigation of anomalous activity.	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - PNM Resources - Public Service Company of New Mexico - 1,3 - WECC,Texas RE	
Answer	
Document Name	
Comment	
It is unclear why the SDT did not incorporate the proposed CIP-007 R6 Requirement into already existing Standards. Logging and log evaluations could have been added to CIP-007 R4, and malicious/anomalous activity capturing and evaluation could have been added to CIP-007 R3. With regards to CIP-007-X R6.3, if an entity were to add a new system into its environment, how long would it have to be compliant with creating a new baseline? This is not clear in the proposed Requirement. CIP-007-X R6.6 states, “Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.” What constitutes “sufficient detail and duration”, and how would that be audited?	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI is concerned that in Requirement R6, the phrase “that has bypassed other security controls” is too broad and generic of an objective statement as there are attacks that may bypass “security controls”, such as CIP-006 physical security controls, that INSM will not detect. To address this concern, we suggest either deleting this phrase or changing it to “that has bypassed other electronic security controls”. EEI suggested adding “in Part 6.2” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below) Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.2** with sufficient detail and duration to support the investigation of anomalous activity.	

Technical Rationale Comments

BCSI Implications (see Classification Rationale, Page 3)

For entities that do not have an internal security monitoring center and may desire to use a cloud-based service, or even onsite monitoring tools today that may have cloud-based data analysis components, there needs to be clarity on the BCSI implications of the data. Page 3 of the Technical Rationale states “Ideally, the NSM system would only be designated as BCSI”, which brings into question the impacts of CIP-004 for cloud vendor personnel where a security monitoring service may require provisioned access to “obtain and use” the BCSI in order to perform the security monitoring function and alert the entity to any anomalies it sees in the data received.

Data Collection Methods, Pages 9 through 10

The term “CIP-networked environment” is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document, section "Data Collection Methods," on pages 9 through 10, outlines considerations for data collection which include Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. To address this concern, we suggest that revisions be made to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.

Likes 0	
Dislikes 0	

Response

Dwanique Spiller - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

We support additional commentary as provided by EEI and NSRF.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment	
ITC supports the response submitted by EEI.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports MRO’s NERC Standards Review Forum’s (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1	
Answer	
Document Name	
Comment	
Exelon supports the comments submitted by the EEI for this questions.	
Likes 0	
Dislikes 0	
Response	
Robert Follini - Avista - Avista Corporation - 3	
Answer	
Document Name	
Comment	

Avista agrees with EEI’s comment:

Comments: EEI suggested adding “in Part 6.4” to Requirement R6, part 6.6. consistent with other parts of Requirement R6. (See boldface edits below)

Develop one or more method(s) to retain network communications data and other relevant data collected **in Part 6.4** with sufficient detail and duration to support the investigation of anomalous activity.

Likes 0

Dislikes 0

Response

James Baldwin - James Baldwin On Behalf of: Matt Lewis, Lower Colorado River Authority, 5, 1; - James Baldwin

Answer

Document Name

Comment

In addition to the comments provided above, LCRA would like to bring the following comments to the attention of the of the SDT:

- There are concerns around real time monitoring and the requirement to respond. There may be instances where personnel are not available to respond to alerting. What is the time requirement around evaluation of alerts?
- The Requirement and Part are written ambiguously and vague. There is concern around the auditability of the new Requirements.
- In the OT environment, a Baseline of traffic may take a long time to develop. Certain events, like winter storms, may result in false flags that could cause unnecessary alerts during emergencies.
- When discussing CIP-Networked Environments, are separate VLANs considered to be a part of the CIP-network.
- What evidence would be required to demonstrate a baseline? Would it be required to export a configuration of the baseline from the INSM?

Likes 0

Dislikes 0

Response

Alain Mukama - Hydro One Networks, Inc. - 1

Answer

Document Name

Comment

The technical rational and guidance need more clarity to align auditors and implementors.

INSM system will have to meet the definition of EACMS as it performs electronic access monitoring function. It is unclear why there was an option not to classify it as EACMS but only BCSI. Clarity is required.

Likes 0

Dislikes 0

Response

Katrina Lyons - Georgia System Operations Corporation - 4

Answer

Document Name

Comment

Part 6.6 necessitates an explicit definition of data retention requirements. The current specification, which mandates retention with "sufficient detail and duration to support the investigation of anomalous activity," introduces a potential challenge. The determination of what constitutes sufficient detail and the appropriate duration is contingent upon the detection and subsequent investigation of anomalous activity. This approach poses a risk of non-compliance in scenarios where anomalous activity is identified after the data has been discarded.

To mitigate this risk, it is advisable to allow for flexibility in retention periods, tailored to the specific nature of the data. For instance, considering the substantial volume of packet captures, it may not be pragmatic to retain them for extended periods. A more nuanced approach that accommodates variations in retention periods for different types of data would enhance practicality and adherence.

We recommend consolidating the proposed Requirements into one or two cohesive Requirements. Additionally, GSOC believes that addressing this requirement within the framework of CIP-005 may be a viable and more streamlined alternative. This consolidation and alignment could contribute to a more coherent and manageable regulatory framework

Likes 0

Dislikes 0

Response

Teresa Krabe - Lower Colorado River Authority - 5, Group Name LCRA Compliance

Answer

Document Name

Comment

In addition to the comments provided above, LCRA would like to bring the following comments to the attention of the SDT:

- There are concerns around real time monitoring and the requirement to respond. There may be instances where personnel are not available to respond to alerting. What is the time requirement around evaluation of alerts?
- The Requirement and Part are written ambiguously and vague. There is concern around the auditability of the new Requirements.
- In the OT environment, a Baseline of traffic may take a long time to develop. Certain events, like winter storms, may result in false flags that could cause unnecessary alerts during emergencies.
- When discussing CIP-Networked Environments, are separate VLANs considered to be a part of the CIP-network?
- What evidence would be required to demonstrate a baseline? Would it be required to export a configuration of the baseline from the INSM?

Likes 0

Dislikes 0

Response

Christine Kane - WEC Energy Group, Inc. - 3, Group Name WEC Energy Group

Answer

Document Name

Comment

WEC Energy Group supports MRO’s NERC Standards Review Forum’s (NSRF) comments.

Likes 0

Dislikes 0

Response

Vicky Budreau - Santee Cooper - 3, Group Name Santee Cooper

Answer

Document Name

Comment

There are some concerns about CIP-007-X R6.3, how often does an entity analyze the traffic? Is it weekly, monthly, or would an instant alert be required. Without a little more direction an auditor and entity may disagree on the frequency.

Likes 0

Dislikes 0

Response

Tristan Miller - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer

Document Name

Comment

The term “CIP-networked environment” is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document section "Data Collection Methods" (on pages 9 through 10) outlines considerations for data collection, which includes Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. CEHE suggests that the SDT make revisions to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.

Likes 0

Dislikes 0

Response

Colby Galloway - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF, Group Name Southern Company

Answer

Document Name

Comment

Scope of Requirement Parts: The SDT has a diagram of many EACMS and PACS communications with various forms of communication either in or out of scope represented by blue/red arrows.   Southern Company suggests the diagram is not clearly represented in the requirement part scope language. For example, the diagram says the communications within a PACS out to its controllers is not in scope, however the requirement scope only states that PACS are in scope (those that rely upon an EACMS for access control). Once a PACS meets that condition, then the entirety of the PACS is in scope, which includes its distributed controllers as the requirement part itself explicitly says “between applicable Cyber Assets” within these systems (the PACS definition only excludes the badge readers, etc. at individual doors). That could be hundreds of widely distributed controllers across the enterprise in scope of this INSM requirement because the PACS is in scope and the main sentence of the requirement is written to “visibility between all applicable Cyber Asset” level, not the system level. There are huge implications of the Cyber Asset granularity rather than monitoring the communications to/from the PACS as a singular system. The SDT diagram is based on communications between systems, but the scoping of the requirement is visibility of all the applicable Cyber Assets within those systems and thus all communications to or from each individual programmable electronic device are in scope. While it states 100% is not required, it seems it is then left as an exercise to the entity to prove why they do not monitor 100% if they only monitor the PACS database server for example. This construct is quite prone to differences of opinion and perceived risk in audits.

As another example, only EACMS that perform access control functions are in scope, but once in scope, then the visibility of all communications between all of its applicable Cyber Assets are in scope, thus all the arrows to any such EACMS are included. The scoping in the standard tells the entity what systems are in scope, but then its focus is monitoring the networks on which those systems reside which will include all comms to/from those systems. It is unclear in the scoping language how that allows for the red “out of scope” arrows.

Southern Company suggests that the requirements be left at the BCS, EACMS, and PACS level, without mention of Cyber Asset within the requirement part language, which would more clearly allow entities the flexibility to monitor to the level of granularity within these systems that provides monitoring value commensurate with the expense and reliability impact of individual components. In the PACS example, the greatest security monitoring value may be for the database server containing the access rights database, but little value in monitoring hundreds of distributed controllers controlling individual doors in facilities across the entity’s footprint. We suggest this would help avoid the “monitor all, but 100% is not required” concept in the current language.

Part 6.2: Southern Company suggests this requirement part is unnecessary (it is covered by 6.6), raises many questions, and adds evidence burden with no direct reliability benefit. It is a necessary step in the monitoring *process*, but not a security objective for a standard. We suggest stating the expected result of INSM rather than step by step procedural "how". Explicitly requiring a "collect the needed data" as a requirement requires not only an evidence burden, but brings with it all the questions of missing data, temporarily malfunctioning equipment, data retention to prove the logging is 100% complete, etc. We suggest deletion of this part.

Overall: Are all security objectives for the internal network inside the ESP also required of the systems outside the ESP in the "CIP Networked Environment?" For example, if the EACMS or PACS in scope are on the corporate network, does CIP-007 R6 require the detection of new devices or connections on the corporate network as well?

Vendor Support: This section of the Technical Rationale and SDT presentations explicitly denies any "per system capability" or allowance for vendor issues where they may not allow for modification of tightly engineered and integrated control systems that are maintained and/or warranted by the vendor. The statements that entities should upgrade due to monitoring requirements, where many control system upgrades at plant locations can begin in the $250,000 range and up, we suggest are overreach into large business/operational decisions that should be made by site management in view of all reliability risks that are being managed. With 6.1 currently stating 100% is not required, it seemed odd to have these "no exceptions based on vendor or system capability" type statements in the TR documentation that further cloud what is a compliant scope.

Examples: Southern Company suggests something that will greatly help the entities understand the INSM requirements is to lay out an example of a 1500MW Combined Cycle generation unit that has medium impact BCS, such as 3 separate multi-layered gas turbine control systems for 3 gas turbines, a different multi-layered turbine control system for a heat recovery steam turbine/generator, and a multi-layered DCS for Balance of Plant (BOP) operations – each of these a multi-layer Perdue model system all on one generating unit. Another example that would help is a large, 1500MW+ offshore wind farm with 200+ individual wind turbines. Thinking through examples such as these and what would be a compliant INSM implementation will help the SDT with scoping requirement parts such as 6.1 as well as helping the industry and CMEP personnel understand what a compliant INSM implementation is, not just in data centers and substation control houses, but in the large industrial plant scenarios within the BES.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

The term "CIP-networked environment" is inclusive of "routable communications" between CIP categorized systems. The CIP-007-X Technical Rational document section "Data Collection Methods" (on pages 9 through 10) outlines considerations for data collection, which includes Layer 2 traffic, which is non-routable. The inclusion of Layer 2 communications contradicts the intended scope of a "CIP-networked environment" and may unintentionally expand the scope of CIP-007-X to include non-routable communications. SIGE suggests that the SDT make revisions to the Technical Rationale document to clarify "routable communications" and update the examples in the "Data Collection Methods" for alignment.

Likes 0	
Dislikes 0	

Response

Lindsay Wickizer - Berkshire Hathaway - PacifiCorp - 6	
Answer	
Document Name	

Comment

We appreciate the approach the SDT took in drafting this standard revision to focus on outcomes without undue proscription or limitations in execution. We hope these offered refinements and considerations will help speed us to an affirmative ballot.

For Part 6.1 we wonder if there is any intentional overlap regarding CIP-012 communications between control centers. Internal network security monitoring between applicable Cyber Assets would seem to preclude communications between control centers. Will the SDT please explain if CIP-012 communications are included under the 6.1 phrase “network communications between applicable Cyber Assets,” or does this language exclude CIP-012 communications? Could we add the qualifying word “internal” between “Identify” and “network?”

Although the webinar explained (at 30:57) that there is no minimum duration imposed on the logging required in Part 6.2, the lack of a specified threshold leaves 6.2 unbounded, leaving Responsible Entities responsible for retaining all logged data for the evidence retention period under C.1.2. There needs to be a reasonable limit defined similar to how the logging requirement of 4.1 is specifically referenced and limited by 4.3. Could we simply add “from Part 6.2” after “data collected” in Part 6.6 to make what is implied clear as was done in Parts 6.4 and 6.5?

The data retention requirement in Requirement 6.6 is open to subjective judgement and second-guessing by any auditor. If Part 6.2 is not modified as suggested and Part 6.6 is retained, please replace the ending period with a comma and add “as determined by the documented processes or procedures of the Responsible Entity.”

Please replace the Measure for Part 6.2 with the language from the Technical Rationale: “When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to: Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic; Forwarding log information to a searchable database for retention; or Summarizing logs in a searchable database.

Part 6.7 uses the term “adversary.” We feel this is a loaded term that is not needed. Deleting “by an adversary” would not diminish data protection.

Regarding CIP-008, We urge the drafting team to include requirement language making it clear that at some point, if investigation of anomalous activity indicates an actual attack or attempt to compromise, that CIP-007 R6 ends and CIP-008 requirements take over. We understand that that is the intent of the drafting team – that CIP-007 R6 could lead into CIP-008 – but the requirement language so far does not indicate that clearly and instead allows for potential of overlap in compliance obligations. The proposed requirement language needs to be clarified to address this point.

Lastly, we thank the SDT for their industry outreach, and hopes we can continue such collaboration as this draft is revised to hopefully reduce ballot iteration and come more quickly to consensus.

Likes 0	
Dislikes 0	

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	

Document Name	
Comment	
ERCOT joins the comments filed by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Megan Melham - Decatur Energy Center LLC - 5	
Answer	
Document Name	
Comment	
We are concerned with the statements the SDT has included in the Technical Rationale regarding Vendor Support where they state on page 4: “Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.” The SDT stating that “every control system should have the capability to provide an appropriate level of visibility” and suggesting that entities will need to update them with modern equipment is unreasonable and may present new risks through new attack vector points into previously isolated systems. This is also in direct contradiction to Requirement R6.1 that allows the entity to assess what level of INSM provides “security value”. Without providing a minimum threshold for monitoring or further guidance on what provides “security value”, there is a lot of room for interpretation into what is required for an entity to meeting compliance with Requirement R6. For those entities that are operating in regulated environments, there is also the possibility of negatively impacting rate payers through costs associated with stranded assets. Including communication between EACMS and PACS systems within the scope of the requirement can create additional obstacles where the systems are managed separately on different networks. There is no guidance provided on how to treat INSM devices that could act as a possible bridge between networks, which would impact compliance with CIP-005.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 3	
Answer	
Document Name	
Comment	

Exelon is responding in support of the comments provided by EEI.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
No other comments	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Alan Kloster On Behalf of: Jeremy Harris, Evergy, 3, 5, 1, 6; Kevin Frick, Evergy, 3, 5, 1, 6; Marcus Moor, Evergy, 3, 5, 1, 6; Tiffany Lake, Evergy, 3, 5, 1, 6; - Alan Kloster	
Answer	
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #11.	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	EEI Near Final Draft Comments _ Project 2023-03 INSM Draft 1 Rev 0d 1_16_2024.docx
Comment	

See comments submitted by the Edison Electric Institute	
Likes 0	
Dislikes 0	
Response	