Comment Report

Project Name:	2023-03 Internal Network Security Monitoring | SAR
Comment Period Start Date:	4/6/2023
Comment Period End Date:	5/5/2023
Associated Ballots:	

There were 37 sets of responses, including comments from approximately 114 different people from approximately 88 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope, please provide your recommendation and explanation.

2. Provide any additional comments for the SAR drafting team 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
WEC Energy Group, Inc.	Christine Kane	3,4,5,6		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
Tacoma Public Utilities (Tacoma, WA)	Jennie Wike	1,3,4,5,6	WECC	Tacoma Power	Jennie Wike	Tacoma Public Utilities	1,3,4,5,6	WECC
					John Merrell	Tacoma Public Utilities (Tacoma, WA)	1	WECC
					John Nierenberg	Tacoma Public Utilities (Tacoma, WA)	3	WECC
					Hien Ho	Tacoma Public Utilities (Tacoma, WA)	4	WECC
					Terry Gifford	Tacoma Public Utilities (Tacoma, WA)	6	WECC
					Ozan Ferrin	Tacoma Public Utilities (Tacoma, WA)	5	WECC
MRO	Jou Yang	1,2,3,4,5,6	MRO	MRO NSRF	Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
					Chris Bills	City of Independence, Power and Light Department	5	MRO
					Fred Meyer	Algonquin Power Co.	3	MRO
					Christopher Bills	City of Independence Power & Light	3,5	MRO
					Larry Heckert	Alliant Energy Corporation Services, Inc.	4	MRO
					Marc Gomez	Southwestern	1	MRO

						Power Administration		
					Matthew Harward	Southwest Power Pool, Inc. (RTO)	2	MRO
					Bryan Sherrow	Board of Public Utilities	1	MRO
					Terry Harbour	Berkshire Hathaway Energy - MidAmerican Energy Co.	1	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Shonda McCain	Omaha Public Power District	6	MRO
					George E Brown	Pattern Operators LP	5	MRO
					George Brown	Acciona Energy USA	5	MRO
					Jaimin Patel	Saskatchewan Power Cooperation	1	MRO
					Kimberly Bentley	Western Area Power Administration	1,6	MRO
					Jay Sethi	Manitoba Hydro	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
FirstEnergy - FirstEnergy Corporation	Mark Garza	1,3,4,5,6		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy -	5	RF

						FirstEnergy Solutions		
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC) Project 2023-03 INSM SAR	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
					Elizabeth Davis	PJM	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					Jim Howell, Jr.	Southern Company - Southern Company Generation	5	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC

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
					Quintin Lee	Eversource Energy	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	1	NPCC

						Authority		
					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
					John Hastings	National Grid	1	NPCC
					Michael Jones	National Grid USA	1	NPCC
NiSource - Northern Indiana Public Service Co.	Steve Toosevich	1,3,5,6		NIPSCO Compliance	Steven Taddeucci	NiSource - Northern Indiana Public Service Co.	3	RF
					Kathryn Tackett	NiSource - Northern Indiana Public Service Co.	5	RF
					Joseph OBrien	NiSource - Northern Indiana Public Service Co.	6	RF

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope, please provide your recommendation and explanation.

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

Answer	No
Document Name	

Comment

PNM does not agree with the proposed scope as described in the SAR.

While PNM agrees that Internal Network Security Monitoring (INSM) for high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC) is important, it is unclear what “forward-looking, objective based” requirements are or would look like without understanding what the specifics of these requirements would be. PNM is hesitant that Standards geared toward implementing INSM controls could become more prescriptive in nature instead of offering guidance on allowable models and controls for entities to consider in determining INSM models for their specific and unique environments.

Order No. 887 refers to a zero-trust architecture as being “fundamental” in INSM. PNM agrees but requests clarity on the definition and scope of zero-trust as it would function in meeting INSM requirements. Zero trust could refer to good network segmentation. It could also refer to a more comprehensive re-building of a network from scratch. The scope of this project could vary greatly depending on industry interpretation of and the necessity to use a zero-trust environment.

PNM also agrees with the comments put forth by EEI that if new requirements were to be put in place, they would need to be risk-based.

Likes 0	
Dislikes 0	

Response

Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The MRO NSRF suggests the detailed description section be modified with additional details to help guide the standard drafting team and help them measure the success of the project. This section contains the following text:

“First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment.”

The use of the term “baseline” could restrict the choice of a vendor based on how their technology was implemented. The associated compliance

evidence for the baseline of network traffic could further restrict technological options if output of this baseline is required. The detailed description also does not clearly articulate the scope of the SAR to focus on high impact Cyber Assets and medium impact Cyber Assets with External Routable Connectivity. The MRO NSRF suggests the following wording:

"First, any new of modified CIP Reliability Standards should address the need for responsible entities to analyze network traffic in an Electronic Security Perimeter (ESP) in between high impact Cyber Assets and medium impact Cyber Assets with External Routable Connectivity (ERC). An anomaly-based analysis is required, where a model of normal network traffic is created and potential malicious traffic is identified based on this model."

The detailed description provides a list of required detections:

"Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment."

The MRO NSRF requests that additional details be added for the required detection of software. Internal network security monitoring does not involve analysis of Cyber Assets themselves and new requirements should not overlap with existing requirements in CIP-010.

The following text is suggested:

"Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software network traffic such as changes to communication protocols in use"

The detailed description also contains the following scoping requirement:

"And third, any new or modified CIP Reliability Standards should require responsible entities to identify anomalous activity to a high level of confidence by…"

The MRO NSRF suggests that the term "to a high level of confidence" be removed. In a zero-defect compliance environment, the requirement to prove a high level of confidence is difficult as it is a subjective statement.

The MRO NSRF suggests that the related standards be modified. The CIP-008 standard should be included in the list as potentially impacted. This will allow the standard drafting team to consider the handling of detected Cyber Security Incidents and ensure this is compatible with requirements for the Cyber Security Incident Response Plan. The CIP-007 standard should be included in the list as potentially impacted as well. This standard already contains requirements for security event monitoring and any standard modifications should be compatible with existing requirements and avoid duplicating requirements. It is unclear why CIP-013 is included in the SAR, the MRO NSRF asks for additional clarity in the SAR, if in fact CIP-013 is to

remain in the SAR scope	
Likes 0	
Dislikes 0	

Response

Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC, Group Name Tacoma Power	
Answer	No
Document Name	

Comment

Tacoma Power does not agree with the proposed scope in the SAR. Below is a summary of Tacoma Power's recommended changes to the SAR scope.

1. Tacoma Power recommends deleting the following bolded language from the last sentence in the Industry Need section in the SAR: "Current CIP Reliability Standards are insufficient to protect against insider threats **or vulnerabilities that are exploited through supply chain attacks such as SolarWinds**." The CIP Standards did protect against the SolarWinds supply chain attack, because the Requirements were sufficient to prevent this attack from affecting the BES reliability. Tacoma Power is concerned that the wording of this SAR implies there were BES reliability impacts from the SolarWinds event. Additionally, the INSM Requirements would provide more protections for threats beyond supply chain, so this statement is not necessary.
2. Tacoma Power proposes that the scope of Project 2023-03 be limited to medium impact BES Cyber Systems at a Control Center. Inbound and outbound malicious communication detection is not yet required in CIP-005 for medium impact BES Cyber System with ERC. INSM is also easier to implement in a Control Center environment than a substation. If FERC Order 887 requires detection of malicious communication at substations, then Tacoma Power recommends that this detection be limited to inbound and outbound detection instead of INSM. This SAR is proposing to skip the step of developing new CIP-005 R1.5 Requirements for inbound and outbound malicious communication detection for medium impact BES Cyber Systems with ERC, and immediately implement INSM.
3. In the Detailed Description section of the SAR, Tacoma Power is concerned with the following numerical items: "(1) logging network traffic (note that packet capture is one means of accomplishing this goal); (2) maintaining logs and other data collected regarding network traffic; and (3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices." These three items are not sufficient on their own to implement an INSM. For example, logging network traffic doesn't support INSM. Tacoma Power recommends deleting these three items.If the Detailed Description remains as written, Tacoma Power recommends that the Detailed Description be expanded to include a description of the objective of capturing and storing the logged data. Ultimately, the objective of INSM is that entities have a process to detect malicious activity inside the CIP network.
4. Tacoma Power recommends deleting Interchange Coordinator and Interchange Authority from the Applicability section of the SAR, as follows: "Applicability will be the same as current CIP standards - Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, Transmission Owner"

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	No
Document Name	

Comment
FE supports EEI's comments and would recommend CIP-008 for inclusion in the scope of this project.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	No
Document Name	

Comment
The scope of the SAR describes the objectives well and contains good details. Manitoba Hydro suggests the detailed description section be modified with some additional details to help guide the standard drafting team and help them measure the success of the project. This section contains the following text: "First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment." The use of the term "baseline" could restrict the choice of a vendor based on how their technology was implemented. The associated compliance evidence for the baseline of network traffic could further restrict technological options if output of this baseline is required. The detailed description also does not clearly articulate the scope of the SAR to focus on high impact Cyber Assets and medium impact Cyber Assets with External Routable Connectivity. Manitoba Hydro suggests the following wording: "First, any new of modified CIP Reliability Standards should address the need for responsible entities to analyze network traffic in an Electronic Security Perimeter (ESP) in between high impact Cyber Assets and medium impact Cyber Assets with External Routable Connectivity (ERC). An anomaly-based analysis is required, where a model of normal network traffic is created and potential malicious traffic is identified based on this model." The detailed description provides a list of required detections: "Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment." Manitoba Hydro requests that additional details be added for the required detection of software. Internal network security monitoring does not involve analysis of Cyber Assets themselves and new requirements should not overlap with existing requirements in CIP-010. The following text is suggested: "Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software network traffic such as changes to communication protocols in use" Manitoba Hydro suggests that the related standards be modified. The CIP-008 standard should be included in the list as potentially impacted. This will allow the standard drafting team to consider the handling of detected Cyber Security Incidents and ensure this is compatible with requirements for the Cyber Security Incident Response Plan. The CIP-007 standard should be included in the list as potentially impacted as well. This standard already contains requirements for security event monitoring and any standard modifications should be compatible with existing requirements and avoid

duplicating requirements. It is unclear why CIP-013 is included in the SAR, Manitoba Hydro asks for additional clarity in the SAR, if in fact CIP-013 is to remain in the SAR scope.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO

Answer	No
Document Name	

Comment

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

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

EEI agrees with the intended scope of the SAR, however, some of the language used in this SAR, while closely aligned with the language in FERC Order 887, does not align with the scoping language for a NERC Reliability Standard. To address these concerns, we offer the following:

1. Project Scope Section: The last sentence in this section should be deleted because it adds no additional insights or direction to the SDT regarding the project scope. Moreover, the scope of the Commission's directives are clear and concise. This sentence in the SAR is a directive for NERC and outside the scope for this project.
2. Detailed Description Section: While the language contained in this section closely aligns with the Commission's Directives, changes are necessary to ensure the directions provided to the SDT are clear, unambiguous and align with NERC's Results Based Standards processes. We additionally note that while we did not delete the phrase "**to a high level of confidence**" in our suggested changes to the Detailed Description section, we do not support changes to the Reliability Standard that are not risk-based. Our proposed changes are as identified in boldface below (deletions not shown because SBS does not accept strikethrough text):

Detail Description Section: Create new or modified CIP Reliability Standards that are **risk**-based and address the need for responsible entities to **utilize security processes, systems and tools that 1)** develop baselines of network traffic inside **an Electronic Security Perimeter; 2)** monitor **for** and detect unauthorized activity, connections, devices, and software inside **an Electronic Security Perimeter; 3) are capable of** identify**ing** anomalous activity to a high level of confidence by (a) logging network traffic **(b**) maintaining logs and other data collected **on** network traffic, **and (c) includes processes that are capable of protecting** evidence from compromised devices**. so that mitigations can be developed to improve responsible entity security against future similar attacks.**

3. Section addressing related Standards or SARs:

i. EEI agrees that close coordination will be needed between the Project 2016-02 SDT and this SDT.

ii. Project 2019-03 should be struck from the list of Projects this SDT will need to coordinate. This project is no longer an active project.

iii EEI agrees the SDT should assess for any impacts to CIP-005 and CIP-010, largely due to possible impacts related to changes in definitions. However, we also believe that CIP-007 should also be included for the reasons identified in our comments.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Evergy - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

Evergy supoprts and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #1.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - AES - AES Corporation - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	No
Document Name	

Comment

AES Clean Energy supports MRO NSRF's comments on this Unofficial Comment Form - see below.

"The MRO NSRF suggests the detailed description section be modified with additional details to help guide the standard drafting team and help them measure the success of the project. This section contains the following text:

'First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment.'

The use of the term 'baseline' could restrict the choice of a vendor based on how their technology was implemented. The associated compliance evidence for the baseline of network traffic could further restrict technological options if output of this baseline is required. The detailed description also does not clearly articulate the scope of the SAR to focus on high impact Cyber Assets and medium impact Cyber Assets with External Routable

Connectivity. The MRO NSRF suggests the following wording:

'First, any new of modified CIP Reliability Standards should address the need for responsible entities to analyze network traffic in an Electronic Security Perimeter (ESP) in between high impact Cyber Assets and medium impact Cyber Assets with External Routable Connectivity (ERC). An anomaly-based analysis is required, where a model of normal network traffic is created and potential malicious traffic is identified based on this model.'

The detailed description provides a list of required detections:

'Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment.'

The MRO NSRF requests that additional details be added for the required detection of software. Internal network security monitoring does not involve analysis of Cyber Assets themselves and new requirements should not overlap with existing requirements in CIP-010.

The following text is suggested:

'Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software network traffic such as changes to communication protocols in use.'

The detailed description also contains the following scoping requirement:

'And third, any new or modified CIP Reliability Standards should require responsible entities to identify anomalous activity to a high level of confidence by…'

The MRO NSRF suggests that the term 'to a high level of confidence' be removed. In a zero-defect compliance environment, the requirement to prove a high level of confidence is difficult as it is a subjective statement.

The MRO NSRF suggests that the related standards be modified. The CIP-008 standard should be included in the list as potentially impacted. This will allow the standard drafting team to consider the handling of detected Cyber Security Incidents and ensure this is compatible with requirements for the Cyber Security Incident Response Plan. The CIP-007 standard should be included in the list as potentially impacted as well. This standard already contains requirements for security event monitoring and any standard modifications should be compatible with existing requirements and avoid duplicating requirements. It is unclear why CIP-013 is included in the SAR, the MRO NSRF asks for additional clarity in the SAR, if in fact CIP-013 is to remain in the SAR scope.

Likes 0	
Dislikes 0	

Response

Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy supports the comments of EEI and the MRO NSRF.

Likes 0	
Dislikes 0	

Response

Brandon Smith - APS - Arizona Public Service Co. - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	

AZPS agrees with the intended scope of the SAR, however also agrees with EEI's suggested changes to the "Detailed Description Section" as identified below:

a. Detail Description Section: Create new or modified **existing** CIP Reliability Standards that are **risk**-based and address the need for responsible entities to **utilize security processes, systems and tools that 1)** develop baselines of network traffic inside **an Electronic Security Perimeter; 2)** monitor **for** and detect unauthorized activity, connections, devices, and software inside **an Electronic Security Perimeter; 3) are capable of** identify**ing** anomalous activity to a high level of confidence by (a) logging network traffic **(b**) maintaining logs and other data collected **on** network traffic, **and (c) includes processes that are capable of protecting** evidence from compromised devices**. so that mitigations can be developed to improve responsible entity security against future similar attacks.**

These recommended changes simplify the scope language and align with existing NERC Reliability Standards.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3,4,5,6, Group Name WEC Energy Group	
Answer	No
Document Name	
Comment	

WEC Energy Group appreciated the opportunity to comment and is in general support of EEI's prepared comments with the following suggested modifications:

The use of the term "baseline", in the Detailed Description Section (item #1), could restrict the choice of a vendor based on how their technology was implemented. The associated compliance evidence for the baseline of network traffic could further restrict technological options if output of this baseline is required. Additionally, the use of the term "baseline" could misalign with the term as used in other Standards like CIP-010.

WEC Energy Group further suggests the following modification based on EEI's prepared comments:
"Create new or modified CIP Reliability Standards that are risk-based and utilize security processes, systems and tools that 1) analyze network traffic inside an Electronic Security Perimeter. Require anomaly-based analysis, where a model of normal network traffic is created and potential malicious traffic is identified based on this model."

Likes 0	

Dislikes 0	
Response	
Justin Welty - NextEra Energy - Florida Power and Light Co. - 1,3,6	
Answer	No
Document Name	
Comment	
NextEra Energy supports EEI's comments.	
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 with the proposed scope of the SAR and supports the comments as submitted by the Edison Electric Institute (EEI).	
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 and Electric (SIGE) does not agree with the proposed scope of the SAR and supports the comments as submitted by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Response	
Lori Frisk - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power agrees with EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Justin Kuehne - AEP - 3,5,6	
Answer	Yes
Document Name	
Comment	
AEP supports the proposed scope as described in the SAR, given that proposed modifications are limited to high impact BES Cyber Systems and medium impact BES Cyber Systems with ERC. Should low impact BES Cyber Systems be included at any point, AEP would have concerns regarding the cost and support required.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Alliant Energy supports the comments submitted by the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	

Alain Mukama - Hydro One Networks, Inc. - 1,3	
Answer	Yes
Document Name	
Comment	
It is recommended to perform the feasibility study to ensure there is adverse impact to the BES reliable operations prior to creating or revising the standards. Also, the project scope should include all ESPs, including the Medium Impact BES Cyber Systems without ERC that are connected in a network.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	Yes
Document Name	
Comment	
Request clarification on this Scope's language which says *The ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges and potential solutions for those BES Cyber systems not in scope.* Does this mean this project's scope may change based on the completed feasibility study? Request clarification on "implementing measures" in part (3) in the Detailed Description, which is different than "monitoring" in parts (1) and (2) "*(3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.*" We believe this language mandates retaining evidence (saving logs). Request clarification of "insider threat" in Industry Need - "*Current CIP Reliability Standards are insufficient to protect against insider threats*" Insider threat could be another CIP Standard or another entity program. We believe this "insider threat" is within the monitored network. The term 'quicker mitigation' should refer to a metric, such as time lapse.	
Likes 0	
Dislikes 0	

Response	
Alison MacKellar - Constellation - 5,6	
Answer	Yes
Document Name	
Comment	
Constellation aligns with Exelon's comments. Alison Mackellar on behalf of Constellation Segments 5 and 6.	
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 membership agrees with the proposed scope of the SAR as it relates to FERC Order 887. The NAGF recommends that the concept under the Detailed Description, “(3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices” be further aligned with the networking security controls intention versus device level security controls.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	Yes
Document Name	
Comment	
Request clarification on this Scope’s language which says "*The ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges and potential solutions for those BES Cyber systems not in scope.".* Does this mean this project’s scope may change based on the completed feasibility study? Request clarification on “implementing measures” in part (3) in the Detailed Description, which is different than “monitoring” in parts (1) and (2): “*(3)*	

implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices." We believe this language mandates retaining evidence (saving logs).

Request clarification of "insider threat" in Industry Need - "*Current CIP Reliability Standards are insufficient to protect against insider threats*"

Insider threat could be another CIP Standard or another entity program. We believe this "insider threat" is within the monitored network.

The term 'quicker mitigation' should refer to a metric, such as time lapse.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 1,3,6

Answer	Yes
Document Name	

Comment

Ameren agrees that the proposed measures are beneficial to the protection of the BES. However, Ameren believes that a phased approach, with the initial focus being on High Impact BES Cyber Systems, would benefit the implementation of INSM technology. High Impact BES Cyber systems are typically centrally located in or near a datacenter and benefit from economies of scale and speed of implementation; whereas, Medium Impact BES Cyber Systems require procurement of hardware, have more complex/niche and interconnected equipment, and are geographically dispersed with a higher volume of site locations, which will require additional time considerations for implementation.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company agrees with the proposed scope in terms of high impact and medium impact BES Cyber Systems with ERC. However, we do offer the following comments detailed in Question 2 for consideration.

Likes 0	
Dislikes 0	

Response

Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the proposed scope as described in the SAR, as the language is directly from FERC Order 887.	
Likes 0	
Dislikes 0	
Response	
Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes
Document Name	
Comment	
MidAmerican agrees with the Project Scope while supporting MRO NSRF and EEI comments regarding the Detailed Description.	
Likes 0	
Dislikes 0	
Response	
Jesus Calderon-Acevedo - Orlando Utilities Commission - 1 - SERC	
Answer	Yes
Document Name	
Comment	
As currently proposed, OUC believes the SAR drafting team should provide more information which addresses concerns regarding the proposed items that are being directed by FERC. When considering the drafting of the requirements as they relate to the creation and monitoring of a network baseline, the drafting team should clearly define what items are to be a part of the baseline along with how often baselines should be monitored and updated. Details regarding actionable items on baseline deviations need to also be clearly stated. There are concerns with whether or not the idea is to achieve 0% packet loss which would be unfeasible, as opposed to collecting a representative sample of network traffic. Additionally, there need to be clear regulations on outage periods for network monitoring to ensure that entities can conduct necessary maintenance and testing on the assets responsible for performing these functions without concern for falling into a state of non-compliance due to a temporary outage, whether it be scheduled or un-scheduled. The expectations regarding the amount of network traffic being captured and requirements on allowances for outages in monitoring (for testing/maintenance) must also be clearly defined. Considerations must also be had on the concerns regarding the monitoring of any real-time communications, as introducing this level of monitoring to systems that rely on low latency	

transmissions may see unintended impacts.

The SAR drafting team should ensure they consider the impacts on the classification of current non-CIP assets that are being used to monitor network traffic and the other requirements they may be beholden to should they need to be classified as CIP assets as this will have an increased impact on managing the OT environment and complying with additional standards such as CIP-004-7, CIP-007-6, CIP-010-4.

When drafting the requirements for the logging of network traffic, the drafting team needs to ensure reasonable limitations are put in place on the retention period of network logs due to the large amount of data that is generated by network traffic in order to avoid unnecessary burdens on entities when it comes to allocating storage for the purpose of maintaining these network logs.

Likes 0	
Dislikes 0	

Response

Donna Wood - Tri-State G and T Association, Inc. - 1,3,5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Israel Perez - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable

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) Project 2023-03 INSM SAR	
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	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steve Toosevich - NiSource - Northern Indiana Public Service Co. - 1,3,5,6, Group Name NIPSCO Compliance	
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	
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	

Request clarification on this Scope's language which says

The ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges, and potential solutions for those BES Cyber systems not in scope.

Does this mean this project's scope may change based on the completed feasibility study?

Request clarification on "implementing measures" in part (3) in the Detailed Description, which is different than "monitoring" in parts (1) and (2)

"*(3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.*"

We believe this language mandates retaining evidence (saving logs).

Request clarification of “insider threat” in Industry Need -

“*Current CIP Reliability Standards are insufficient to protect against insider threats*”

Insider threat could be another CIP Standard or another entity program. We believe this “insider threat” is within the monitored network.

Likes 0	
Dislikes 0	

Response

2. Provide any additional comments for the SAR drafting team to consider, if desired.

Joseph Amato - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	
Document Name	

Comment

MidAmerican agrees with the Project Scope while supporting MRO NSRF and EEI comments regarding the Detailed Description.

MidAmerican is concerned that a requirement to baseline network traffic may be inadvisably prescriptive, forestalling other potentially effective approaches. Also, a network traffic baseline would likely be a proprietary product of any INSM software, and not something that could be exported to satisfy evidencing requirements.

We are also concerned about the SAR directing a requirement to identify anomalous activity "to a high level of confidence." We don't see how a requirement could be drafted to a subjective level of performance and respectfully request removal of this phrase.

Likes 0	
Dislikes 0	

Response

Christine Kane - WEC Energy Group, Inc. - 3,4,5,6, Group Name WEC Energy Group

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

Industry Need section

The phrase “to ensure the detection of anomalous network activity indicative of an attack in progress” is used. We suggest that this is a desirable goal,

but no technology or standard can 100% *ensure* this. As the next sentence in the SAR states, it may "increase the probability of early detection". We suggest removing/replacing the "to ensure" in this scoping document.

In that same section, we suggest rewording or removing broad statements like "Current CIP Reliability Standards are insufficient to protect against insider threats or vulnerabilities that are exploited through supply chain attacks such as SolarWinds." As this INSM SAR is a scoping document for a standards development project and SDTs often refer to their SAR to answer scope questions, we suggest this clearly focus the team's scope to the specific issue at hand – detecting potential malicious activity on these networks that may have bypassed the ESP/EAP layer of defense. This scoping document should not state or imply the SDT's scope is to protect against all insider threats or address all aspects of supply chain vulnerabilities. As a team with a defined deadline, clear and concise scoping will be needed that supports the team in avoiding scope creep.

Purpose or Goal section

This section does not address how the proposed project provides the reliability-related benefit, as the heading indicates, but is instead an implementation scope statement. We would suggest that the purpose or goal of how INSM provides the reliability benefit will be of importance to the SDT as they work under a regulatory deadline on such a large and involved topic.

Related Standards or SARs section

We find that Project 2019-03 was completed at the end of 2020 and no longer exists. We suggest removal of that project from this section and in its place add the Project 2023-04 SAR which will be addressing "detection of malicious communications to/between assets containing low impact BES Cyber Systems with external routable connectivity" to insure coordination on these related topics. Project 2022-05 is also working on issues relating to "attempts to compromise" and some degree of coordination may be needed there. There are many concurrent CIP standard activities with impacts to each other.

We suggest close coordination with Project 2016-02 as it is also making forward-looking changes to CIP-005. Those changes affect this INSM project at least in these ways:

• 2016-02 is modifying the associated definitions (ESP/EAP/ERC) and Requirements to no longer prescribe the perimeter-based "castle/moat" network architecture only and enable Zero Trust-based architectures. That project is proposing removing all "internal/inside" and "external/outside" terminology and replacing it with "protected by" to better align with and allow for ZT architectures while remaining backward compatible. As this SAR and project have "internal network" in the name, coordination is necessary. Also, as the principle of ZT that no network is trusted comes to fruition and all network traffic is encrypted, this impacts the ability to monitor at the network layer. As the ZT principles also work to shrink the "ESP" down to an individual workload/container/device rather than a network, the concept of "internal" will need coordination with 2016-02 as it also works to make the CIP standards incorporate these forward-looking options.

• 2016-02 is also addressing what is known as the "SuperESP" issue to remove impediments to the capability of seamlessly moving executing virtual servers from one location to another (e.g., primary to backup data center). Therefore 2016-02 is adding encryption requirements for portions of an "internal network" when a single ESP extends between different locations (though not using terms like inside/internal). The INSM SDT will need to coordinate with those changes as well.

As to the individual CIP standards mentioned in the SAR's scope, we understand CIP-005's inclusion for INSM, however the tie to CIP-010 concerning configuration management of an individual system and CIP-013 for supply chain procurement processes is unclear. We suggest that a review of CIP-007 R4's "Security Event Monitoring" may need to be included (see discussion concerning Zero Trust above) as well as CIP-008 with its "attempts to

compromise” concepts and requirements.

It is for these reasons that we suggest INSM may become more host/hypervisor/policy engine based in the future rather than “on the wire” packets as networks incorporate more end-to-end encryption and that CIP-007 (and its R4 Security Event Monitoring) would have a more direct tie to this SAR and need to be included.

We suggest making note of these (at a high level) in the SAR so these overlapping issues with 2016-02, 2023-04, and 2022-05 are known and coordinated.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 1,3,6

Answer	
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

SPP supports the comments submitted by the SRC and MRO NSRF.

SPP would ask the SDT to consider the potential cost that may arise from the scope of this SAR. 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 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 potential 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	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy supports the comments of the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - AES - AES Corporation - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	
Document Name	
Comment	
AES Clean Energy supports MRO NSRF's comments on this Unofficial Comment Form - see below. "The MRO NSRF suggests that the title of the SAR be updated to 'Electronic Security Perimeter Internal Network Security Monitoring' to better reflect the scope of the SAR applicable to High impact Cyber Assets and Medium impact Cyber Assets with External Routable Connectivity (ERC)."	
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	
Request consideration of cloud-based monitoring solutions.	
Likes 0	

Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
ERCOT joins the comments submitted by the ISO/RTO Council Standards Review Committee	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	
Document Name	
Comment	
Request consideration of cloud-based monitoring solutions.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	
Document Name	
Comment	
MPC supports comments submitted by the MRO NERC Standards Review Forum (NSRF).	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) Project 2023-03 INSM SAR	
Answer	
Document Name	
Comment	
The IRC SRC supports the forward-looking, objective-based approach in the SAR for addressing the three goals outlined in the SAR. The eventual drafting team will need to provide clear definitions of what constitutes a “baseline” to establish anomalous activity. Responsible entities will need that clarification in order to determine what changes are going to be required (if any) to establish and maintain compliance with the new or revised standard/s.	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network and Security Technologies - 1 - NA - Not Applicable	
Answer	
Document Name	
Comment	
NST suggests the Standard Drafting Team be tasked with considering whether internal network connections used for time-sensitive protection or control functions between intelligent electronic devices be exempted from new "INSM" requirements in order to avoid potential problems caused by INSM latency.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	
Document Name	
Comment	
Manitoba Hydro suggests that the title of the SAR be updated to “Electronic Security Perimeter Internal Network Security Monitoring” to better reflect the scope of the SAR applicable to High impact Cyber Assets and Medium impact Cyber Assets with External Routable Connectivity (ERC).	

Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	
Document Name	
Comment	
N/A	
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	
Alison MacKellar - Constellation - 5,6	
Answer	
Document Name	
Comment	
Constellation aligns with Exelon's comments. Alison Mackellar on behalf of Constellation Segments 5 and 6.	
Likes 0	

Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP agrees with the SAR, however, some additional explanation may be needed as to what is changing, since the information is vague. For example, network traffic is already logged, logs can be used to support incident investigation, implementing measures for maintaining logs and other data can be used for comparison analysis in unlikely event of attacker trying to remove/cover up activity. In addition, what is to be done differently at our Control Centers? Currently, we are already doing what is being proposed, such as logging networking traffic, and maintaining logs and other network traffic data collected, sufficient to draw meaningful conclusions and support incident investigation. Plus, we maintain the integrity of those logs and other data.	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	
Document Name	
Comment	
Request consideration of cloud-based monitoring solutions.	
Likes 0	
Dislikes 0	
Response	
Larry Heckert - Alliant Energy Corporation Services, Inc. - 4	
Answer	
Document Name	
Comment	

N/A	
Likes 0	
Dislikes 0	
Response	
Jennie Wike - Tacoma Public Utilities (Tacoma, WA) - 1,3,4,5,6 - WECC, Group Name Tacoma Power	
Answer	
Document Name	
Comment	
When drafting the Standard and implementation guidance, Tacoma Power recommends that the SDT consider entities who have implemented a zero trust environment. For these entities, the implementation of INSM is unneccassary because there is no trusted network that requires monitoring.	
Likes 0	
Dislikes 0	
Response	
Jou Yang - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The MRO NSRF suggests that the title of the SAR be updated to “Electronic Security Perimeter Internal Network Security Monitoring” to better reflect the scope of the SAR applicable to High impact Cyber Assets and Medium impact Cyber Assets with External Routable Connectivity (ERC).	
Likes 0	
Dislikes 0	
Response	