Comment Report

Project Name:	2022-05 Modifications to CIP-008 Reporting Threshold | SAR
Comment Period Start Date:	11/2/2022
Comment Period End Date:	12/5/2022
Associated Ballots:	

There were 37 sets of responses, including comments from approximately 96 different people from approximately 72 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. Do you believe that other CIP standards will need to be modified for consistency to meet the goals laid out in the SAR? If so, please provide the standard recommendation and explanation

3. 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
Eversource Energy	Joshua London	1,3		Eversource	Joshua London	Eversource Energy	1	NPCC
					Vicki O'Leary	Eversource Energy	3	NPCC
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 - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC) Project 2022-05 Modifications to CIP-008	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

					Andrew Gallo	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
					Sheraz Majid	Hydro One Networks, Inc.	1	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					John Hastings	National Grid	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Chantal Mazza	Hydro Quebec	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

Dan Kopin	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
Nicolas Turcotte	Hydro-Qu?bec TransEnergie	1	NPCC
Randy MacDonald	New Brunswick Power Corporation	2	NPCC
Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
Michael Jones	National Grid	3	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
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC

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.

Kinte Whitehead - Exelon - 1,3

Answer	No
Document Name	

Comment

Exelon supports the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1,3

Answer	No
Document Name	

Comment

Exelon supports the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) Project 2022-05 Modifications to CIP-008

Answer	No
Document Name	

Comment

The definition of "Attempt to Compromise" should reference the methods used in CIP-005-7 R1.5 and CIP-007-6 R4.2 to define thresholds to establish an "Attempt to Compromise" and therefore a Cyber Security Incident. The SRC recommends using these criteria as the defining thresholds as opposed to additional language in CIP-008.

Establishing minimum criteria for managing intent should be part of the scope of this SAR. Thresholds may be helpful but, we don't believe that this will significantly change the items that are deemed "reportable."

The tracking of security information for sources like E-ISAC is expensive (resource-wise). Adding additional events that are culled from the responses to this standard would increase that burden.

Many CIP assets are not internet facing. Suggesting that these expectations for number of reportable incidents should not be based on internet related metrics. The SRC recommends avoiding over-reporting.

The SRC requests an update to submit to only the E-ISAC with the E-ISAC sharing with NCCIC.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The SAR does not justify a need for a minimum reporting threshold other than to say that NERC's "...study concluded that the current language of the Reliability Standard permits the use of subjective criteria to define attempt(s) to compromise, and most programs include a provision allowing a level of staff discretion." It is not clear whether or not this study determined that cyber security incidents were not being reported.

Generally, if a SAR cites a white paper or study, the white paper or study is included on the project page. This study should be posted for the consideration of industry and to help us better understand the need for this SAR. MPC cannot agree with the scope of this SAR without understanding how this SAR supports reliability.

Likes 0	
Dislikes 0	

Response

Paul Mehlhaff - Sunflower Electric Power Corporation - 1

Answer	No
Document Name	

Comment

Sunflower opposes creating a minimum threshold for reporting requirements on attempts to compromise, as required in CIP-008-6 R1.2. Delineating and reporting on Cyber Security Incidents and attempts to compromise is an important part of any Registered Entity's security program; entities cannot defend their systems without constant vigilance and analysis. However, there are several reasons that the MRO NSRF believes that instituting a minimum threshold is not needed and may do more harm to BES reliability than good. Each of these reasons is discussed below but in summary they are:

1) Erroneous emphasis on quantity of reporting as an indicator of improved cyber security; and

2) Imposition of an arbitrary minimum reporting threshold over the professional opinions of those Subject Matter Experts who are best educated, knowledgeable, and equipped to recognize and respond to potential attempts to compromise or Cyber Security Incidents.

The driving – in fact, only argument – that the SAR makes for revising CIP-008 is that there was no increase in the number of reports filed once CIP-008-5 was replaced by CIP-008-6. Specifically, the SAR document states, “Since the effective date of CIP-008-6 there has not been a material change in the number of Reportable Cyber Security Incidents or Cyber Security Incidents that were determined to be an attempt to compromise an applicable system.” This argument is based on the unstated assumption that there must have been an increase in reports mandated by CIP-008-6. Further, the SAR document states that CIP-008-6 became effective January 1, 2021. It also states that NERC began its study of the impacts of implementing that standard in third quarter of 2021. This seems a short period of time to make sweeping statements regarding the effectiveness of a newly-revised standard.

We do not know the causes behind the current number of reports filed or if there should be fewer, more, or if the number currently reported is accurate based on the actual incidents that have occurred. The SAR does not address these questions at all. It makes a flat statement that since the number of reports didn’t rise, then therefore the current standard version is flawed. There is nothing in the (unstated) number of reports to justify that sweeping generalization.

If the ERO is going to argue that there need to be more CIP-008 reports, or that it expects a minimum number per year, what is that number? If NERC wanted the industry to file more reports under CIP-008 when enacting CIP-008-6, what was the target number of additional that it sought? One? Two? 100? If the industry is going to be held to a quota, the ERO should at least be transparent and indicate what that number is and what it’s based on.

Methods of monitoring and investigating used are vastly different across entities. This is due to diversity in architecture, types of in-scope assets, the structure of the security organization, the size of the company, the amount of traffic seen across IT and OT networks, and many other variables. Designing a monitoring and reporting program must take all of this into account to be effective.

Take as an example an entity that has an Electronic Access Point on a firewall that also has an interface exposed to the internet. In this case, reporting port scans and brute force attempts originating from internet hosts may be relevant to CIP-008 reporting. A different entity may have multiple layers of firewalls and other security controls between an EAP and the internet, such that traffic arriving at an internet-facing firewall is completely irrelevant to the security posture of the in-scope CIP assets and their associated CIP-008 reporting criteria. It would be extremely difficult to design a "minimum expectation threshold" applicable across all Registered Entities that allows for such a variety of system implementations without either excluding relevant events for some or placing undue burden with little security benefit on others.

In NERC’s study report on CIP-008, as well as within the SAR document, NERC repeatedly criticizes CIP-008-6 for relying on the subjective criteria of Registered Entities for determining what an attempt to compromise is. “Subjective criteria” is not a pejorative. A registered entity’s subject matter experts are the best authority for determining the impact of an event on their company.

Another important area to consider is other reporting requirements outside NERC CIP, especially for combined electric/natural gas entities as well as those with nuclear assets. Each of these areas (NERC CIP, TSA, NRC) has associated event reporting requirements. Allowing latitude such that entities can define specific reportable event criteria allows for standardization across all compliance areas, which results not only in decreasing burden

on operators but more importantly a standardized process and smaller set of criteria for security teams to train on and effectively implement. Different reporting requirements leading to analyst confusion cannot be discounted as a significant barrier to effective program implementation.

The ability of security groups to be self-identifying and nimble in determining, investigating, addressing, and reporting attempts to compromise increases effectiveness and security. Conversely, taking valuable and limited resources to perform those same activities on standardized minimum criteria that may not actually be deemed a creditable threat will surely cause ineffectiveness and reduce security.

Lastly, we would point out that even in NERC's June 27, 2022 assessment of CIP-008-6, the assessment that drove this SAR, NERC itself points out that industry cyber security experts are addressing the risks and have implemented necessary security practices. The assessment states, "Based on responses provided, most registered entities have processes and internal controls around the detection, review, coordination, and reporting of cyber security incidents. Also, most entities use advanced detection tools, and the staff is sufficiently trained in incident detection and response." Despite NERC's acknowledgment of the industry's effectiveness in preventing attempts to compromise on internal OT networks, NERC has requested additional administrative activities that may result in lowering the established security effectiveness already in place.

In closing, the NERC Reliability Standards are risk-based. This SAR does not identify the risk and should be rejected on that ground. If NERC feels there is a risk from not having more reports filed under CIP-008, it must demonstrate that to the industry through data and evidence.

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 North American Generator Forum (NAGF) would like to express three main concerns of its membership:

1. Project 2022-05 SAR and the future SDT should take into consideration the wider Federal efforts to increase critical infrastructure owners and operators reporting of cyber security incidents. The NAGF membership is sensitive to the fact that increased reporting requirements enforced by multiple agencies at the same time may be duplicative in nature and an ineffective additional burden on the individual organizations. The overall result may be a reduction in the effectiveness of information sharing.

2. The SAR implies that there is a direct correlation between the number of reports submitted and the effectiveness of the reporting requirements in CIP-008-6. The NAGF membership cautions that there is not enough information that has been publicly circulated to ascertain if a correlation between the number of reports submitted and the standards effectiveness is objectively established.

NAGF noted that:

a. Network architectures utilizing Defense-in-Depth practices sequester the ESP and EACMS from direct exposure to the internet and publicly accessible areas of the network. Therefore, a reduced number of “attempted intrusions” and Reportable Cyber Security Incidents is the result of attacks being limited to those originating within the organizational wide area network (WAN) or secured areas of the organizational WAN.

b. The current CIP-008-6 reporting requirements Applicable Systems in Table R1 are the appropriately scoped NERC Cyber Security Incident reporting systems. Cyber Security Incidents that occur within the organization but without impacting the ESP and EACMS should only be reported on a discretionary basis.

3. Any criteria developed should continue to employ risk-based analysis of attempted intrusions by the organizations prior to the establishment of a specific incident being deemed Reportable.

Likes 0	
Dislikes 0	

Response

Karen Demos - NextEra Energy - Florida Power and Light Co. - 1,3,6

Answer	No
Document Name	

Comment

NextEra Energy (NEE) supports the specific comments, included below, submitted by the Electric Edison Institute: “EEI does not support the SAR scope because a technical basis to support the SAR was not provided to allow industry to understand the gap this SAR is trying to address. The summary report stated that “most registered entities have processes and internal controls around the detection, review, coordination, and reporting of cyber security incidents.” It also states that “most entities use advanced detection tools, and the staff is sufficiently trained in incident detection and response,” all of which indicates that CIP-008-6 is performing in a manner that mitigates the risk to the reliable operation of the BES. This conflicting information does not support the need to modify CIP-008-6.

It is important that NERC recognize that while delineating and reporting on Cyber Security Incidents and attempts to compromise is an important part of any responsible entity's security program, the consistent reporting does not in of itself indicate a problem. Industry utilizes a defense in depth strategy and detects and stops attempts at enterprise boundaries before they ever reach internal ESPs or control networks, including EACMS and PACS, around our most critical control systems.

We also note that the methods of monitoring and investigating under entity Cyber Security Incident response plans vastly differ across entity networks. This is due to the diversity in architecture, types of in-scope assets, the structure of the security organization, the size of the company, the amount of traffic seen across IT and OT networks, and many other variables. Resulting in a need for entities to have the ability to design their monitoring and reporting programs without regulatory burdens that do not consider these differences. For this reason, we caution against the development of a one size fits all solutions that is overly prescriptive in design that may weaken the protections already in place within entity networks.

Additionally, consideration must be given to the fact that many entities have reporting obligations outside of the NERC CIP Reliability Standard, noting many entities manage systems that include electric, natural gas and nuclear assets. Each of these areas (NERC CISA, TSA, NRC, DOE, etc.) has associated event reporting requirements. Allowing latitude such that entities can define specific reportable event criteria allows for standardization and harmonization across all compliance areas, which results not only in decreasing burden on operators but more importantly a standardized process and valuable set of criteria for security teams to train on and effectively implement. Different reporting requirements can lead to analyst confusion and reporting errors.

For all of the above reasons, we ask that NERC reconsider the appropriateness of this SAR.”

Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	No
Document Name	
Comment	

GRE opposes creating a minimum threshold for reporting requirements on attempts to compromise, as required in CIP-008-6 R1.2. Delineating and reporting on Cyber Security Incidents and attempts to compromise is an important part of any Registered Entity's security program; entities cannot defend their systems without constant vigilance and analysis. However, there are several reasons that the GRE believes that instituting a minimum threshold is not needed and may do more harm to BES reliability than good. Each of these reasons is discussed below but in summary they are:

1) Erroneous emphasis on quantity of reporting as an indicator of improved cyber security; and

2) Imposition of an arbitrary minimum reporting threshold over the professional opinions of those Subject Matter Experts who are best educated, knowledgeable, and equipped to recognize and respond to potential attempts to compromise or Cyber Security Incidents.

The driving – in fact, only argument – that the SAR makes for revising CIP-008 is that there was no increase in the number of reports filed once CIP-008-5 was replaced by CIP-008-6. Specifically, the SAR document states, “Since the effective date of CIP-008-6 there has not been a material change in the number of Reportable Cyber Security Incidents or Cyber Security Incidents that were determined to be an attempt to compromise an applicable system.” This argument is based on the unstated assumption that there must have been an increase in reports mandated by CIP-008-6. Further, the SAR document states that CIP-008-6 became effective January 1, 2021. It also states that NERC began its study of the impacts of implementing that standard in third quarter of 2021. This seems a short period of time to make sweeping statements regarding the effectiveness of a newly-revised standard.

We do not know the causes behind the current number of reports filed or if there should be fewer, more, or if the number currently reported is accurate based on the actual incidents that have occurred. The SAR does not address these questions at all. It makes a flat statement that since the number of reports didn’t rise, then therefore the current standard version is flawed. There is nothing in the (unstated) number of reports to justify that sweeping generalization.

If the ERO is going to argue that there need to be more CIP-008 reports, or that it expects a minimum number per year, what is that number? If NERC wanted the industry to file more reports under CIP-008 when enacting CIP-008-6, what was the target number of additional that it sought? One? Two? 100? If the industry is going to be held to a quota, the ERO should at least be transparent and indicate what that number is and what it’s based on.

Methods of monitoring and investigating used are vastly different across entities. This is due to diversity in architecture, types of in-scope assets, the structure of the security organization, the size of the company, the amount of traffic seen across IT and OT networks, and many other variables. Designing a monitoring and reporting program must take all of this into account to be effective.

Take as an example an entity that has an Electronic Access Point on a firewall that also has an interface exposed to the internet. In this case, reporting port scans and brute force attempts originating from internet hosts may be relevant to CIP-008 reporting. A different entity may have multiple layers of firewalls and other security controls between an EAP and the internet, such that traffic arriving at an internet-facing firewall is completely irrelevant to the security posture of the in-scope CIP assets and their associated CIP-008 reporting criteria. It would be extremely difficult to design a "minimum expectation threshold" applicable across all Registered Entities that allows for such a variety of system implementations without either excluding relevant events for some or placing undue burden with little security benefit on others.

In NERC's study report on CIP-008, as well as within the SAR document, NERC repeatedly criticizes CIP-008-6 for relying on the subjective criteria of Registered Entities for determining what an attempt to compromise is. "Subjective criteria" is not a pejorative. A registered entity's subject matter experts are the best authority for determining the impact of an event on their company.

Another important area to consider is other reporting requirements outside NERC CIP, especially for combined electric/natural gas entities as well as those with nuclear assets. Each of these areas (NERC CIP, TSA, NRC) has associated event reporting requirements. Allowing latitude such that entities can define specific reportable event criteria allows for standardization across all compliance areas, which results not only in decreasing burden on operators but more importantly a standardized process and smaller set of criteria for security teams to train on and effectively implement. Different reporting requirements leading to analyst confusion cannot be discounted as a significant barrier to effective program implementation.

The ability of security groups to be self-identifying and nimble in determining, investigating, addressing, and reporting attempts to compromise increases effectiveness and security. Conversely, taking valuable and limited resources to perform those same activities on standardized minimum criteria that may not actually be deemed a creditable threat will surely cause ineffectiveness and reduce security.

Lastly, we would point out that even in NERC's June 27, 2022 assessment of CIP-008-6, the assessment that drove this SAR, NERC itself points out that industry cyber security experts are addressing the risks and have implemented necessary security practices. The assessment states, "Based on responses provided, most registered entities have processes and internal controls around the detection, review, coordination, and reporting of cyber security incidents. Also, most entities use advanced detection tools, and the staff is sufficiently trained in incident detection and response." Despite NERC's acknowledgment of the industry's effectiveness in preventing attempts to compromise on internal OT networks, NERC has requested additional administrative activities that may result in lowering the established security effectiveness already in place.

In closing, the NERC Reliability Standards are risk-based. This SAR does not identify the risk and should be rejected on that ground. If NERC feels there is a risk from not having more reports filed under CIP-008, it must demonstrate that to the industry through data and evidence.

Likes 0	
Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

We support EEI's comments.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We ask the SDT to provide a more prescriptive definition for "attempt to compromise" will not materially increase the level of reporting. "Attempt to compromise" should be defined in the NERC Glossary of Terms. This will help us when reporting if we witness attempts to compromise the ESP or EACMS. We would like more clarity for what the SDT is trying to address in the volume of reports.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

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

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	No
Document Name	

Comment

Request update to submit to only the E-ISAC with the E-ISAC sharing with NCCIC/CISA.

Consider different paths. Here are four paths.

1) Expand the scope and define the scope of “attempt to compromise”. In this path, recommend defining “attempt to compromise.” Suggest this definition reference the methods and threshold used in CIP-005-6 R1.5 and CIP-007-6 R4.2 . . . thereby a Cyber Security Incident.

2) Do not need this update because the family of CIP Standards work. Many CIP assets are not internet facing. Suggest these expectations should not be based on internet metrics. Recommend avoiding over-reporting. Proposed changes may not result in expected metrics.

Previous SDT tried to define “attempt to compromise.” That industry feedback did not agree on an industry wide definition.

May be premature to update CIP-008 with coming CERCIA – see CISA RFI. Should CIP-008 be consistent with CISA reporting?

3) Should the CIP-008 objective switch to pre-incident? If YES, can CIP-008 metrics switch from a lagging to leading indicator?

It may be easier to define security event instead of “attempts to compromise.” Instead of incident reporting, change to reporting security events. This new approach avoids the difficulty in defining “attempt” and/or “suspicious.” This new approach avoids different interpretations.

Likes 0	
Dislikes 0	

Response

Joshua London - Eversource Energy - 1,3, Group Name Eversource

Answer	No
Document Name	

Comment

Eversource agrees with the comments of EEI and the NPCC.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5

Answer	No
Document Name	

Comment

Request update to submit to only the E-ISAC with the E-ISAC sharing with NCCIC/CISA.

Consider different paths. Here are four paths.

1)Expand the scope and define the scope of “attempt to compromise”. In this path, recommend defining “attempt to compromise.” Suggest this definition reference the methods and threshold used in CIP-005-6 R1.5 and CIP-007-6 R4.2 . . . thereby a Cyber Security Incident.

2)Do not need this update because the family of CIP Standards work. Many CIP assets are not internet facing. Suggest these expectations should not be based on internet metrics. Recommend avoiding over-reporting. Proposed changes may not result in expected metrics.

Previous SDT tried to define “attempt to compromise.” That industry feedback did not agree on an industry wide definition.

May be premature to update CIP-008 with coming CERCIA – see CISA RFI. Should CIP-008 be consistent with CISA reporting?

3)Should the CIP-008 objective switch to pre-incident? If YES, can CIP-008 metrics switch from a lagging to leading indicator?

It may be easier to define security event instead of “attempts to compromise.” Instead of incident reporting, change to reporting security events. This new approach avoids the difficulty in defining “attempt” and/or “suspicious.” This new approach avoids different interpretations.

Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern agrees with EEI's assessment.	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
NPPD does not see a need for this SAR. The existing standard provides adequate flexibility for an entity to determine appropriate reporting for their environment. The lack of reports can be for many reasons. In our case we feel it is due to the layered security protective equipment used prior to BES protective equipment to minimize the risk to the BES and thus greatly reduces any potential attack. This in turn greatly reduces the associated reporting.	
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 the SAR scope because a technical basis to support the SAR was not provided to allow industry to understand the gap this SAR is trying to address. The summary report stated that "most registered entities have processes and internal controls around the detection, review, coordination, and reporting of cyber security incidents." It also states that "most entities use advanced detection tools, and the staff is sufficiently trained	

in incident detection and response," all of which indicates that CIP-008-6 is performing in a manner that mitigates the risk to the reliable operation of the BES. This conflicting information does not support the need to modify CIP-008-6.

It is important that NERC recognize that while delineating and reporting on Cyber Security Incidents and attempts to compromise is an important part of any responsible entity's security program, the consistent reporting does not in of itself indicate a problem. Industry utilizes a defense in depth strategy and detects and stops attempts at enterprise boundaries before they ever reach internal ESPs or control networks, including EACMS and PACS, around our most critical control systems.

We also note that the methods of monitoring and investigating under entity Cyber Security Incident response plans vastly differ across entity networks. This is due to the diversity in architecture, types of in-scope assets, the structure of the security organization, the size of the company, the amount of traffic seen across IT and OT networks, and many other variables. Resulting in a need for entities to have the ability to design their monitoring and reporting programs without regulatory burdens that do not consider these differences. For this reason, we caution against the development of a one size fits all solutions that is overly prescriptive in design that may weaken the protections already in place within entity networks.

Additionally, consideration must be given to the fact that many entities have reporting obligations outside of the NERC CIP Reliability Standard, noting many entities manage systems that include electric, natural gas and nuclear assets. Each of these areas (NERC CISA, TSA, NRC, DOE, etc.) has associated event reporting requirements. Allowing latitude such that entities can define specific reportable event criteria allows for standardization and harmonization across all compliance areas, which results not only in decreasing burden on operators but more importantly a standardized process and valuable set of criteria for security teams to train on and effectively implement. Different reporting requirements can lead to analyst confusion and reporting errors.

It is also important to note that CISA is currently seeking input as it develops proposed regulations required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"). Among other things, CIRCIA directs CISA to develop and oversee implementation of regulations requiring covered entities to submit to CISA reports detailing covered cyber incidents and ransom payments. Rather than duplicate efforts or creating conflicting requirements, NERC should coordinate with CISA, which will result in decreasing burdens on operators but more importantly provide standardized processes and valuable sets of criteria for security teams to train and effectively implement.

For all of the above reasons, we ask that NERC reconsider the appropriateness of this SAR.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The definition of "Attempt to Compromise" should reference the methods used in CIP-005-6 R1.5 and CIP-007-6 R4.2 to define thresholds to establish an "Attempt to Compromise" and therefore a Cyber Security Incident. SPP recommends using these criteria as the defining thresholds as opposed to additional language in CIP-008.

Establishing minimum criteria for managing intent should be part of the scope of this SAR. Thresholds may be helpful but, we don't believe that this will significantly change the items that are deemed "reportable."

The tracking of security information for sources like E-ISAC is expensive (resource-wise). Adding additional events that are culled from the responses to this standard would increase that burden.

Many CIP assets are not internet facing. Suggesting that these expectations for number of reportable incidents should not be based on internet related metrics. SPP recommends avoiding over-reporting.

SPP requests an update to submit to only the E-ISAC with the E-ISAC sharing with CISA

Likes 0	
Dislikes 0	

Response

Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CEHE) believes that a proposed scope change, as defined in the SAR, is not necessary to reflect accurate reporting of an “Attempt to Compromise.” The benefit of the existing language is that each entity is afforded the opportunity to define an “Attempt to Compromise” that fits its environment and therefore report actual, malicious activities that have the potential to threaten the system.

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 opposes creating a minimum threshold for reporting requirements on attempts to compromise, as required in CIP-008-6 R1.2. Delineating and reporting on Cyber Security Incidents and attempts to compromise is an important part of any Registered Entity's security program; entities cannot defend their systems without constant vigilance and analysis. However, there are several reasons that we believe that instituting a minimum threshold is not needed and may do more harm to BES reliability than good. Each of these reasons is discussed below but in summary they are:

1. Erroneous emphasis on quantity of reporting as an indicator of improved cyber security; and
2. Imposition of an minimum reporting threshold over the professional opinions of those Subject Matter Experts who are best educated, knowledgeable, and equipped to recognize and respond to potential attempts to compromise or Cyber Security Incidents.

The perceived driving argument this SAR makes for revising CIP-008 is that there was no increase in the number of reports filed once CIP-008-5 was replaced by CIP-008-6. Specifically, the SAR document states, “Since the effective date of CIP-008-6 there has not been a material change in the number of Reportable Cyber Security Incidents or Cyber Security Incidents that were determined to be an attempt to compromise an applicable system.” This argument is based on the unstated assumption that there must have been an increase in reports mandated by CIP-008-6. Further, the SAR document states that CIP-008-6 became effective January 1, 2021. It also states that NERC began its study of the impacts of implementing that

standard in third quarter of 2021. This seems a short period of time to make statements regarding the effectiveness of a relatively newly-revised standard.

We do not know the causes behind the current number of reports filed or if there should be fewer, more, or if the number currently reported is accurate based on the actual incidents that have occurred. The SAR does not address these questions at all. It makes a general statement that since the number of reports didn't rise, then therefore the current standard version is flawed. There is nothing in the (unstated) number of reports to justify that generalization.

If the ERO is going to argue that there needs to be more CIP-008 reports, or that it expects a minimum number per year, what will that justified number be? If NERC wanted the industry to file more reports under CIP-008 when enacting CIP-008-6, what was the target number? If the industry is going to be held to a quota, the ERO should indicate what that number is and what it's based on.

Methods of monitoring and investigating used are vastly different across entities. This is due to diversity in architecture, types of in-scope assets, the structure of the security organization, the size of the company, the amount of traffic seen across IT and OT networks, and many other variables. Designing a monitoring and reporting program must take all of this into account to be effective.

Take as an example an entity that has an Electronic Access Point on a firewall that also has an interface exposed to the Internet. In this case, reporting port scans and brute force attempts originating from Internet hosts may be relevant to CIP-008 reporting. A different entity may have multiple layers of firewalls and other security controls between an EAP and the Internet, such that traffic arriving at an internet-facing firewall is separate to the security posture of the in-scope CIP assets and their associated CIP-008 reporting criteria. It would be extremely difficult to design a "minimum expectation threshold" applicable across all Registered Entities that allows for such a variety of system implementations without either excluding relevant events for some or placing undue burden with little security benefit on others.

Another important area to consider is other reporting requirements outside NERC CIP, especially for combined electric/natural gas entities as well as those with nuclear assets. Each of these areas (NERC CIP, TSA, NRC) has associated event reporting requirements. Allowing latitude such that entities can define specific reportable event criteria allows for standardization across all compliance areas, which results not only in decreasing burden on operators but more importantly a standardized process and smaller set of criteria for security teams to train on and effectively implement. Different reporting requirements leading to analyst confusion cannot be discounted as a significant barrier to effective program implementation.

In NERC's study report on CIP-008, as well as within the SAR document, NERC repeatedly suggests CIP-008-6 is flawed for relying on the subjective criteria of Registered Entities for determining what an attempt to compromise is. "Subjective criteria" relies on the registered entity's subject matter experts who are the best authority for determining the impact of an event on their company. The ability of security groups to be self-identifying and nimble in determining, investigating, addressing, and reporting attempts to compromise increases effectiveness and security. Conversely, taking valuable and limited resources to perform those same activities on standardized minimum criteria that may not actually be deemed a creditable threat will surely cause ineffectiveness and reduce security.

Lastly, we would point out that even in NERC's June 27, 2022 assessment of CIP-008-6, NERC points out that industry cyber security experts are addressing the risks and have implemented necessary security practices. The assessment states, "Based on responses provided, most registered entities have processes and internal controls around the detection, review, coordination, and reporting of cyber security incidents. Also, most entities use advanced detection tools, and the staff is sufficiently trained in incident detection and response." Despite NERC's acknowledgment of the industry's effectiveness in preventing attempts to compromise internal OT networks, NERC is proposing additional administrative activities that may result in lowering the established security effectiveness already in place.

In closing, the NERC Reliability Standards are risk-based. This SAR does not identify the risk and should be rejected on that ground. If NERC feels there is a risk from not having more reports filed under CIP-008, it must demonstrate that to the industry through data and evidence.

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 a proposed scope change, as defined in the SAR, is not necessary to reflect accurate reporting of an “Attempt to Compromise.” The benefit of the existing language is that each entity is afforded the opportunity to define an “Attempt to Compromise” that fits its environment and therefore report actual, malicious activities that have the potential to threaten the system.

Likes 0	
Dislikes 0	

Response

Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	

Comment

Xcel Energy Supports EEI Comments.

In addition to EEI comments, Xcel Energy opposes creating a minimum threshold for reporting requirements on attempts to compromise, as required in CIP-008-6 R1.2. Delineating and reporting on Cyber Security Incidents and attempts to compromise is an important part of any Registered Entity's security program; entities cannot defend their systems without constant vigilance and analysis. However, there are several reasons that Xcel Energy believes instituting a minimum threshold is unnecessary and may create new risks to BES reliability. Our reasons against modifications to reporting criteria are discussed in detail below but are summarized below as:

1) Erroneous emphasis on quantity of reporting as an indicator of improved cyber security; and

2) Imposition of an arbitrary minimum reporting threshold over the professional opinions of those Subject Matter Experts who are best educated, knowledgeable, and equipped to recognize and respond to potential attempts to compromise or Cyber Security Incidents.

The driving, and, in fact only, argument that the SAR makes for revising CIP-008 is that there was no increase in the number of reports filed once CIP-008-5 was replaced by CIP-008-6. Specifically, the SAR document states, “Since the effective date of CIP-008-6 there has not been a material change in the number of Reportable Cyber Security Incidents or Cyber Security Incidents that were determined to be an attempt to compromise an applicable system.” This argument is based on the unstated assumption that there must have been an increase in reports mandated by CIP-008-6. Further, the SAR document states that CIP-008-6 became effective on January 1, 2021. It also states that NERC began its study of the impacts of implementing that standard in the third quarter of 2021. The length of the observation period does support a period in which a good sample can be measured.

The SAR does not address what NERC believes constitutes an acceptable number of notifications of an attempt to compromise to be made by the industry. But rather, it makes a flat statement that since the number of reports didn’t rise, then, therefore, the current standard version is flawed. There is nothing in the (unstated) number of reports to justify that sweeping generalization. If the ERO is going to argue that there need to be more CIP-008 reports, or that it expects a minimum number per year, then that quota should be quantified and supported with proper evidence.

The SAR does not address how minimum reporting criteria would affect each entity very differently. Methods of securing, monitoring, and investigating are vastly different across entities. This is due to diversity in architecture, types of in-scope assets, the structure of the security organization, the size of

the company, the amount of traffic seen across IT and OT networks, and many other variables. Designing a monitoring and reporting program must take all of this into account to be effective.

Take as an example an entity that has an Electronic Access Point on a firewall that also has an interface exposed to the internet. In this case, reporting port scans and brute force attempts originating from internet hosts may be relevant to CIP-008 reporting. A different entity may have multiple layers of firewalls and other security controls between an EAP and the internet, such that traffic arriving at an internet-facing firewall is completely irrelevant to the security posture of the in-scope CIP assets and their associated CIP-008 reporting criteria. It would be extremely difficult to design a "minimum expectation threshold" applicable across all Registered Entities that allows for such a variety of system implementations without either excluding relevant events for some or placing undue burden with little security benefit on others.

In NERC's study report on CIP-008, as well as within the SAR document, NERC repeatedly criticizes CIP-008-6 for relying on the subjective criteria of Registered Entities for determining what an attempt to compromise is. "Subjective criteria" is not a pejorative. A registered entity's subject matter experts are the best authority for determining the impact of an event on their company.

Another important area to consider is other reporting requirements outside NERC CIP, especially for combined electric/natural gas entities as well as those with nuclear assets. Each of these areas (NERC CIP, TSA, NRC) has associated event reporting requirements. Allowing latitude such that entities can define specific reportable event criteria allows for standardization across all compliance areas, which results not only in decreasing burden on operators but more importantly a standardized process and smaller set of criteria for security teams to train on and effectively implement. Different reporting requirements leading to analyst confusion cannot be discounted as a significant barrier to effective program implementation.

The ability of security groups to be self-identifying and nimble in determining, investigating, addressing, and reporting attempts to compromise increases effectiveness and security. Conversely, taking valuable and limited resources to perform those same activities on standardized minimum criteria that may not be deemed a creditable threat will surely cause ineffectiveness and reduce security.

Lastly, we would point out that even in NERC's June 27, 2022 assessment of CIP-008-6, the assessment that drove this SAR, NERC itself points out that industry cyber security experts are addressing the risks and have implemented necessary security practices. The assessment states, "Based on responses provided, most registered entities have processes and internal controls around the detection, review, coordination, and reporting of cyber security incidents. Also, most entities use advanced detection tools, and the staff is sufficiently trained in incident detection and response." Despite NERC's acknowledgment of the industry's effectiveness in preventing attempts to compromise on internal OT networks, NERC has requested additional administrative activities that may result in lowering the established security effectiveness already in place.

In closing, the NERC Reliability Standards are risk-based. This SAR does not identify the risk and should be rejected on that ground. If NERC feels there is a risk from not having more reports filed under CIP-008, it should demonstrate that to the industry through data and evidence.

Likes 0	
Dislikes 0	

Response

Justin MacDonald - Midwest Energy, Inc. - 1

Answer	No
Document Name	

Comment

Midwest Energy opposes creating a minimum threshold for reporting requirements for CIP-008. Our primary reasons for this position are:

1. At this time there does not seem to be a clear connection between increased number of filed reports and improved cyber security (further, NERC has never stated how many reports it expects should be filed on which time basis to be seen as evidence of improved cyber security); and
2. Issues surrounding minimum reporting thresholds. A reporting threshold could potentially be set so low as to require more frequent than initially intended reports. Further, any threshold would neglect the specific attributes of the registered entity in question and the details of any incident they are undergoing.

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

Request update to submit to only the E-ISAC with the E-ISAC sharing with NCCIC/CISA.

Consider different paths. Here are four paths.

1) Expand the scope and define the scope of an “attempt to compromise”. In this path, recommend defining “attempt to compromise.” Suggest this definition reference the methods and threshold used in CIP-005-6 R1.5 and CIP-007-6 R4.2 . . . thereby a Cyber Security Incident.

2) Do not need this update because the family of CIP Standards works. Many CIP assets are not internet-facing. Suggest these expectations should not be based on internet metrics. Recommend avoiding over-reporting. Proposed changes may not result in expected metrics.

Previous SDT tried to define “attempt to compromise.” That industry feedback did not agree on an industry-wide definition.

May be premature to update CIP-008 with coming to CERCIA – see CISA RFI. Should CIP-008 be consistent with CISA reporting?

3) Should the CIP-008 objective switch to pre-incident? If YES, can CIP-008 metrics switch from lagging to a leading indicator?

It may be easier to define security events instead of “attempts to compromise.” Instead of incident reporting, change to reporting security events. This new approach avoids the difficulty of defining “attempt” and/or “suspicious.” This new approach avoids different interpretations.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter

Answer	No
Document Name	

Comment

The justification for the SAR it states "… there has not been a material change in the number of … incidents that were determined to be an attempt to compromise an applicable system" is engaging in a counting exercise in reportability rather than an evaluation of a complex landscape of risks and threats. Mandatory reporting must carefully consider the appropriate utilization of scarce personnel resources in cyber security roles to ensure meaningful security risks are communicated and that those risk are not overshadowed by excessive reporting resulting from unrealistic expectations. Most ESPs and EACMSs within entities are already well-protected with defense-in-depth strategies such that applicable systems are not likely to encounter casual "attempts to compromise" that are in any way meaningful to report. Thus, by definition, such reporting would be minimally statistically significant. For "attempted" cyber attacks to be meaningful to report, they must pass a set of criteria including perceived intent (which is always subjective), exclusion of operational issues (e.g., mis-entered passwords by an otherwise-authorized user, accidental connection attempt to the wrong jump host, etc. etc.), and realistic threat to the BES.

ESPs and EACMSs would not be generally Internet-facing. Thus, the threat of attempted opportunities drops precipitously. Internet-facing systems are persistently subjected to and potentially affected by attempts such as credential stuffing of password-based logons or XSS spraying attacks against websites or any similar "shot-gun" intrusion approach that is not a targeted attack. For an ESP or EACMS residing within what is already a protected perimeter of an entity's corporate network (as an example), to have an attempted compromise of a covered asset requires that a complex chain of events including access gained by an adversary inside of a corporate network (i.e. externally-controlled beach head or an insider threat), identification of a system that would have access through an EAP, and then a credible attack against the system which has the access through the EAP, and then subsequently fails. Quite simply, in an entity that is already performing rigorous defense practices, the realistic number of such reportable attempts is low to non-existent.

Using the SAR to further define attempts will likely result in one of two outcomes – either the definition arising from significant industry debate will essentially match what entities are already applying in good faith to comply with CIP-008-6 resulting in minimal change to the number of reports or the definition will be unworkable resulting in a panoply of false alerts, half-understood events, and outright noise which devalues the entire reporting process and structure.

To accurately determine if additional refinement is in order, the REs' audit results against CIP-008-6 should show that entities are non-compliant or questionably compliant with implementing good-faith procedures for complying with attempted cyber incident reporting. There is no reasonable metric that is based in numbers alone on what the right number of cyber incident reports should be for an industry. Additionally, the need for additional reporting should be supported by facts and data pointing to events that escalated or continued to place the industry at risk based on lack of communication from an initial compromised entity.

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 5,6

Answer	No
Document Name	
Comment	
Constellation aligns with Exelon Corporation and EEI responses to this question Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
There is value in maintaining a level of discretion in interpretation of “attempts to compromise”. The standard applies to a wide variety of environments and technologies, and each entity will have its own architectures and mitigations to consider. The SDT seems to acknowledge that every port scan, phishing email, or endpoint AV alert does not constitute a reportable event. In most cases that will come down to an assessment of intent as well as impact, which often requires some amount of subjective reasoning based on the unique circumstances. Quantitative and qualitative thresholds may result in over reporting of events.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy supports the comments provided by the Edison Electric Institute.	
Likes 0	
Dislikes 0	

Response	
Roger Fradenburgh - Network + Security Technologies - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

NST strongly disagrees with this project's proposed scope and the SAR's assertion the project will "Improve awareness of existing and future cyber security risk to the BES." Adding mandatory, quantitative, threshold-based criteria for "attempts to compromise" to CIP-008 probably would, in fact, result in an increase in the number of reports to the E-ISAC and the NCCIC, which seems to be the real goal here, but we are hard-pressed to see how making incident analysis, response, and reporting procedures formulaic will advance the cause of protecting the BES from malicious cyber actors.

NST is particularly troubled by the fact the SAR is critical of Responsible Entity use of "subjective criteria" and of incident response programs that include provisions "allowing a level of staff discretion." The professional judgment of trained and experienced incident response team members is, we assert, one of the most valuable tools available to incident response team leaders, yet the SAR seems to suggest a better approach to incident response would be to consult a "What do to, when to call" table in a new, improved version of CIP-008.

NST urges NERC to consider the following before deciding to jettison professional judgment:

The third paragraph in the Forward of NERC's 2021 "ERO Compliance Monitoring and Enforcement Manual" reads, "This Manual does not define how to determine compliance with the NERC Reliability Standards. This Manual also does not serve as a substitute for *professional judgment*, training, and experience." (italics added)

Given that NIST standards and guidelines are held in high regard by many FERC, NERC, Regional Entity and Registered Entity personnel, NST consulted its well-thumbed copy of Special Publication SP-800-61r2, "Computer Security Incident Handling Guide," and took note of several statements in Section 3.2.4 ("Incident Analysis"):

"Even if an indicator is accurate, it does not necessarily mean that an incident has occurred. Some indicators, such as a server crash or modification of critical files, could happen for several reasons other than a security incident, including human error. Given the occurrence of indicators, however, it is reasonable to suspect that an incident might be occurring and to act accordingly. *Determining whether a particular event is actually an incident is sometimes a matter of judgment.*" (Italics added)

"Although technical solutions exist that can make detection easier, the best remedy is to build a team of highly experienced and proficient staff members who can analyze the precursors and indicators effectively and efficiently and take appropriate actions. Without a well-trained and capable staff, incident detection and analysis will be conducted inefficiently, and costly mistakes will be made."

NST also disagrees with the idea that reporting thresholds can be "right sized" across the entire spectrum of Registered Entities subject to CIP-008. Cyber events that might be indicators of malicious activity can, and in our experience do, vary from one entity to the next. Baseline, "normal" Cyber Asset CPU utilizations and network traffic levels are similarly variable depending on many factors including time of day, weather, and others. Anomalous activity levels might indicate someone or something is mounting an attack, or they might mean something else entirely. At some Control Centers, X failed login attempts in Y minutes could be an indication of trouble, while at others, it could be a common occurrence.

The SAR notes, "thresholds should not be so prescriptive as to require the reporting of every internet facing firewall port scan, phishing email identified, or file alerted by endpoint anti-virus scans." Fair enough, but how prescriptive should thresholds be? How many internet facing firewall port scans, over what period of time, should require a report? We note that at many BES assets, particularly Control Centers, ESP firewalls are typically not internet-facing, so the only port scans they are likely to see will typically be the result of CIP-010 vulnerability testing. How many phishing emails should be received, over what period of time, by how many individuals, before a report should be submitted? Most Registered Entity email systems are on corporate networks that are not under NERC jurisdiction, so while it might well be helpful for Entities to report significant amounts of phishing activity to the E-ISAC, this is not something CIP-008 can mandate.

NST is also concerned that since the impetus for this SAR is a dearth of "attempts to compromise" reports, there's a risk a drafting team would develop a set of "lowest common denominator" thresholds, established more to ensure wide industry participation in a new reporting regime than to gather useful information about evolving cyber threats.

In summary, NST believes this SAR is attempting to solve a problem that may or may not actually exist, using an approach that risks turning CIP-008 compliance into an unproductive paper chase. If the ERO believes Registered Entities and, by extension, BES reliability, would benefit from having additional guidance about cyber event analysis and about approaches to evaluating indicators of possible malicious activity, this should be all means be pursued, but it should take the form of industry outreach (webinars, white papers, technical training, etc.), not arbitrary revisions to CIP-008 that would replace professional judgement with artificial "thresholds."

Likes 0	
Dislikes 0	

Response

Alison MacKellar - Constellation - 5,6

Answer	No
Document Name	

Comment

Constellation aligns with Exelon Corporation and EEI responses to this question

Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Alexander Brickner - University of Massachusetts Lowell Applied Research Corporation - 9,10 - NPCC

Answer	Yes
Document Name	

Comment

Cybersecurity threats to the United States national and economic security are increasing in frequency, scale, sophistication, and severity of impact. Increasing threats reinforce the growing need for collaboration, communication, and a whole-of-community approach to defending and responding to cyber incidents impacting critical electric infrastructure (CEI) through formalized information sharing partnerships and standards. Communities, comprised of local, territorial, tribal, state, federal and military agencies are responsible for developing and deploying software to rapidly map and deploy cyber-physical infrastructure within critical infrastructure systems to enhance Defense Support of Civil Authorities (DSCA) and other cyber operations.

The Department of Energy (DOE) and Cybersecurity and Infrastructure Security Agency (CISA) created several federal electric-sector cybersecurity programs, including the Cybersecurity Risk Information Sharing Program (CRISP) and the Electricity Information Sharing and Analysis Center (E-ISAC)

that are included in the current CIP cybersecurity reporting standards. These programs are an important first step, However, recent GridEx exercises have demonstrated the need for better coordination with communities as well as federal agencies.

The University of Massachusetts Applied Research Corporation (UMLARC) proposes that communities should be responsible for deploying community cyber infrastructure, in consultation with utilities, to identify vulnerabilities, protect critical energy infrastructure and networks, enable automated assessment, provide situational awareness, and respond to the threats within the electric sector across disparate and siloed cybersecurity platforms at multiple levels of classification. A virtual terrain map and actionable specifications must be continuously maintained, updated by a community cyber force (CCF) to enable effective coordinated response across a diverse array of stakeholders in hours instead of months.

Unfortunately, communities have struggled to implement electric-sector community cyber infrastructure because incident reporting standards are loosely defined and, as a result, are often excluded from security planning. Further, the lack of well-defined standards discourages both public and private investments and limits the deployment of capabilities that are critical to deter, detect, defend, or recover from major cybersecurity threats, including nation state attacks. Updating CIP-008 to include local communities as a recipient of cyber incident reports, in addition to the (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC), provides a unique opportunity for NERC to help both utilities and communities deploy technology, operational capability, and services to enable effective cybersecurity coordination for the bulk power system.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

We support the modification of CIP-008 to create objective criteria for attempts to compromise.

Likes 0	
Dislikes 0	

Response

Lindsey Mannion - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Justin Kuehne - AEP - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	

2. Do you believe that other CIP standards will need to be modified for consistency to meet the goals laid out in the SAR? If so, please provide the standard recommendation and explanation	
Alison MacKellar - Constellation - 5,6	
Answer	No
Document Name	
Comment	
Constellation aligns with Exelon Corporation and EEI responses to this question Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Roger Fradenburgh - Network + Security Technologies - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
As indicated in our response to Question 1, NST does not support the SAR's proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy agrees with EEI comments: “does not support the modifications described for this CIP-008-6 SAR and therefore we do not agree that conformative changes within other CIP Standards is needed or has been demonstrated to address any known reliability gaps.”	
Likes 0	
Dislikes 0	

Response	
Kimberly Turco - Constellation - 5,6	
Answer	No
Document Name	
Comment	
Constellation aligns with Exelon Corporation and EEI responses to this question Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	No
Document Name	
Comment	
Please see our response for Q1. FirstEnergy does not support the modifications described for this CIP-008-6 SAR and therefore do not agree that changes within other CIP Standards is needed.	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	No
Document Name	
Comment	
Midwest Energy does not believe any other CIP standards need to be modified as part of this SAR.	
Likes 0	

Dislikes 0	
Response	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	No
Document Name	
Comment	
No NERC standards should be modified to institute a minimum reporting threshold for attempts to compromise.	
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 additional modifications to other CIP standards is necessary. However, a change in defined incident reporting thresholds may have minimal impact to CIP-003-8: incident reporting and response planning for Low Impact BES Assets. Any modifications to the definition would require that existing controls and measurements be adjusted to reflect those changes.	
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	
As indicated in response to question 1, WEC Energy Group does not believe any modifications to the CIP standards should be made. If the ERO or Regional Entities believe a responsible entity's program of identifying creditable threats to compromise is not as strong as it should be, then recommendations can be made as to how that entity could increase the strength of its program. But standardized criteria for all entities would not be effective.	

Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CEHE does not believe additional modifications to other CIP standards are necessary. However, a change in defined incident reporting thresholds may have minimal impact to CIP-003-8: incident reporting and response planning for Low Impact BES Assets. Any modifications to the definition would require that existing controls and measurements be adjusted to reflect those changes.	
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 the modifications described for this CIP-008-6 SAR and therefore we do not agree that conformative changes within other CIP Standards is needed or has been demonstrated to address any known reliability gaps. While EEI would be quick to support a NERC Reliability Project that intends to close a clear gap in Reliability, we do not support the development of a project without technical justification.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
Southern agrees with EEI’s assessment.	

Likes 0	
Dislikes 0	
Response	
Joshua London - Eversource Energy - 1,3, Group Name Eversource	
Answer	No
Document Name	
Comment	
Eversource agrees with the comments of EEI and the NPCC.	
Likes 0	
Dislikes 0	
Response	
Alan Kloster - Evergy - 1,3,5,6 - MRO	
Answer	No
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) for question #2.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 1,3,6	
Answer	No
Document Name	
Comment	
We believe that the desired modifications around attempt to compromise should be contained within the CIP-008 Standard.	
Likes 0	
Dislikes 0	

Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	No
Document Name	
Comment	
We support EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Great River Energy - 1,3,5,6	
Answer	No
Document Name	
Comment	
As indicated in response to question 1, GRE does not believe any modifications to the CIP standards should be made. If the ERO or Regional Entities believe a responsible entity's program of identifying creditable threats to compromise is not as strong as it should be, then recommendations can be made as to how that entity could increase the strength of its program. But standardized criteria for all entities would not be effective.	
Likes 0	
Dislikes 0	
Response	
Karen Demos - NextEra Energy - Florida Power and Light Co. - 1,3,6	
Answer	No
Document Name	
Comment	
NEE supports the comments submitted by the EEI in their entirety: "EEI does not support the modifications described for this CIP-008-6 SAR and therefore we do not agree that conformative changes within other CIP Standards is needed or has been demonstrated to address any known reliability gaps. While NEE would be quick to support a NERC Reliability Project that intends to close a clear gap in Reliability, we do not support the development of a project without technical justification."	
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 would need additional information to determine if other CIP Standards need to be considered for consistency.	
Likes 0	
Dislikes 0	
Response	
Paul Mehlhaff - Sunflower Electric Power Corporation - 1	
Answer	No
Document Name	
Comment	
As indicated in response to question 1, Sunflower does not believe any modifications to the CIP standards should be made. If the ERO or Regional Entities believe a responsible entity's program of identifying creditable threats to compromise is not as strong as it should be, then recommendations can be made as to how that entity could increase the strength of its program. But standardized criteria for all entities would not be effective.	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1,3	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	

Response	
Kinte Whitehead - Exelon - 1,3	
Answer	No
Document Name	
Comment	
Exelon supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
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	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Bender - Nebraska Public Power District - 1,3,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Carl Pineault - Hydro-Qu?bec Production - 1,5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - MRO,WECC,Texas RE,SERC,RF	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Minnkota Power Cooperative Inc. - 1,5 - MRO	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) Project 2022-05 Modifications to CIP-008	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Justin Kuehne - AEP - 3,5,6	
Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA believes that this is dependent on the outcome of the criteria that will be established. If the new definition establishes criteria that add to additional requirements beyond the applicable parts in CIP-007-6 Table R4, CIP-007-6 could require modification.	
Likes 0	
Dislikes 0	
Response	
Alexander Brickner - University of Massachusetts Lowell Applied Research Corporation - 9,10 - NPCC	
Answer	Yes
Document Name	
Comment	
Yes, “CIP-003-8 - Cyber Security — Security Management Control” should be modified to include references to local community cyber forces as well national cyber response capabilities.	
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	
Document Name	

Comment

In addition to its impact on CIP-008, Texas RE suggests the drafting team review the impact of a definition change of Cyber Security Incident on CIP-007-6 R4 Parts 4.1 and 4.4, CIP-006-6 R1 Parts 1.5, 1.7, and 1.10, and CIP-00-9-6 R1 Part 1.5.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

No Comment

Likes 0	
Dislikes 0	

Response

3. Provide any additional comments for the SAR drafting team to consider, if desired.	
Justin Kuehne - AEP - 3,5,6	
Answer	
Document Name	
Comment	
AEP appreciates the opportunity to review and comment on the SAR for this project. We agree with the need to include more prescriptive language to ensure the proper Cyber Security Incidents are being reported. To accomplish that, AEP recommends that the list of threshold criteria be as comprehensive as possible so that it is clear to Responsible Entities when and what type of Incidents need to be reported.	
Likes 0	
Dislikes 0	
Response	
Kinte Whitehead - Exelon - 1,3	
Answer	
Document Name	
Comment	
Exelon supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Daniel Gacek - Exelon - 1,3	
Answer	
Document Name	
Comment	
Exelon supports the comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response	

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC) Project 2022-05 Modifications to CIP-008

Answer	
Document Name	

Comment

"Attempt to Compromise" should be a defined term within the Glossary of Terms.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Please revise the SAR to support the reliability impact of this change, including any supporting information. Particularly, is NERC aware of any data that demonstrates that cyber security events are being broadly under-reported as a result of the current CIP-008 language and is any potential under-reporting detrimental to reliability on the aggregate?

Likes 0	
Dislikes 0	

Response

Paul Mehlhaff - Sunflower Electric Power Corporation - 1

Answer	
Document Name	

Comment

As stated above, the MRO NSRF does not support this SAR and does not believe it should proceed in its current state. If NERC is absolutely convinced that the Reliability Standard CIP-008-6 must be revised, then NERC should craft a new SAR with new reasoning for it, that get at the actual security concern that needs to be addressed (because number of reports in and of itself is not a security concern). We ask that NERC work directly with industry stakeholders and representatives to identify the concern(s) and potential improvements, so that the next SAR for CIP-008-6 is not imposed on the industry by NERC but that instead represents the consensus and approval of both groups. We thank you for your time and consideration of these comments.

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 at this time.

Likes 0	
Dislikes 0	

Response

Alexander Brickner - University of Massachusetts Lowell Applied Research Corporation - 9,10 - NPCC

Answer	
Document Name	

Comment

More than 98% of military installations located in the United States currently depend on the civilian power grid. As such, force protection operations at military installations are dependent on linked physical and cyber infrastructures. These interconnected infrastructures, while improving capabilities and mission effectiveness, also increase vulnerability to potential failures due to human error, natural disasters, or intentional attack. Threats to American military installations are becoming more complex, covert, and unpredictable due to advancements in technology. Additionally threats to installations are becoming more complex, covert, and unpredictable due to advancements in technology.

Risks are compounded because the Department of Defense (DoD) does not have an organized, outward-facing focus on CEI and lacks the dedicated staff, capabilities, or processes to effectively coordinate cyber incident responses with utility systems. Additionally, implementing software is challenging because there is no central program office that has the vision, authorities, and expertise to drive and execute on the CEI cybersecurity mission. Coordination and collaboration between utilities and the military is a challenge. The stakeholder convening processes to have constructive dialogue around defense energy resilience planning are complex.

The nation’s defense communities are investing in innovative solutions to enable collaboration between electric utilities and local, state, and federal government to anticipate and respond to cyberattacks against critical infrastructure to ensure continuity of operations and mission assurance. For example, UMLARC partnered with the University of Massachusetts Lowell to submit a proposal for a community cyber support facility through the Defense Community Infrastructure Pilot Program (DCIP). On September 23, 2022, the Office of Local Defense Community Corporation (OLDCC) announced $1,278,280 in funding to the University of Massachusetts, Lowell in support of Hanscom Air Force Base to construct a new cyber operations center to support the region during critical incidents.

Likes 0	
Dislikes 0	

Response
Michael Brytowski - Great River Energy - 1,3,5,6
Answer	
Document Name	
Comment
As stated above, GRE does not support this SAR and does not believe it should proceed in its current state. If NERC is absolutely convinced that the Reliability Standard CIP-008-6 must be revised, then NERC should craft a new SAR with new reasoning for it, that get at the actual security concern that needs to be addressed (because number of reports in and of itself is not a security concern). We ask that NERC work directly with industry stakeholders and representatives to identify the concern(s) and potential improvements, so that the next SAR for CIP-008-6 is not imposed on the industry by NERC but that instead represents the consensus and approval of both groups. We thank you for your time and consideration of these comments.
Likes 0	
Dislikes 0	
Response
Andrea Jessup - Bonneville Power Administration - 1,3,5,6 - WECC
Answer	
Document Name	
Comment
For success to be achieved, BPA believes there will have to be agreement on the implementation of some industry accepted framework such as MITRE ATT&CK and its "Initial Access" catalog of techniques to provide both REs and regulators with defined TTPs.
Likes 0	
Dislikes 0	
Response
David Jendras Sr - Ameren - Ameren Services - 1,3,6
Answer	
Document Name	
Comment

For consideration: Ameren defines an "attempt to compromise" as an attempt to gain unauthorized access to data, a system, a network, other electronic assets, or a combination thereof, with the purpose of negatively impacting the accessibility, confidentiality, or integrity of one or more components.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1

Answer	
Document Name	

Comment

“Attempt to Compromise” should be defined in the Glossary of Terms.

Industry has not supported hard to define terms like “suspicious” or “sabotage” such as “attempt to compromise.” Industry wants the same expectations as auditors.

Also, the recent CISA Cyber Incident Reporting muddies this conversation.

Likes 0	
Dislikes 0	

Response

Joshua London - Eversource Energy - 1,3, Group Name Eversource

Answer	
Document Name	

Comment

Eversource agrees with the comments of EEI and the NPCC.

Likes 0	
Dislikes 0	

Response

Carl Pineault - Hydro-Qu?bec Production - 1,5

Answer	

Document Name	
Comment	
“Attempt to Compromise” should be defined in the Glossary of Terms. Industry has not supported hard to define terms like “suspicious” or “sabotage” such as “attempt to compromise.” Industry wants the same expectations as auditors. Also, the recent CISA Cyber Incident Reporting muddies this conversation.	
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	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Navodka Carter - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
CEHE does not support the proposed scope of the SAR because existing NERC CIP requirements are robust and provide controls to help utilities effectively deter bad actors from attempting to compromise the BES. Some alternative suggestions to amending the requirement and definition of “Attempt to Compromise,” are: Drafting Compliance Guidance; this would allow entities the opportunity to continue to approach compliance in a feasible manner, Having entities voluntarily submit annual threat summaries that summarize cybersecurity threats the entity encounters, but effectively thwarts.	

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

SIGE does not support the proposed scope of the SAR because existing NERC CIP requirements are robust and provide controls to help utilities effectively deter bad actors from attempting to compromise the BES.

Some suggestions instead of amending the requirement and definition of “Attempt to Compromise,” are:

- Drafting Compliance Guidance; this would allow entities the opportunity to continue to approach compliance in a feasible manner,
- Having entities voluntarily submit annual threat summaries that summarize cybersecurity threats the entity encounters, but effectively thwarts.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

No Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE supports the addition of a requirement for Registered Entities to define “attempt to compromise” to include, at a minimum, a to be determined prescribed list of items. To the extent the SDT modifies the requirement language in CIP-008, the drafting team should ensure the NERC Glossary terms remain consistent with the requirement language.	
Likes 0	
Dislikes 0	
Response	
Justin MacDonald - Midwest Energy, Inc. - 1	
Answer	
Document Name	
Comment	
Midwest Energy encourages SARs written to directly address new or changing cyber security concerns. Directly addressing cyber security concerns does not include, at this time, a required minimum reporting threshold.	
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	

“Attempt to Compromise” should be defined in the Glossary of Terms.

The industry has not supported hard-to-define terms like “suspicious” or “sabotage” such as “attempt to compromise.” The industry wants the same expectations as auditors.

Also, the recent CISA Cyber Incident Reporting muddies this conversation.

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

Kimberly Turco - Constellation - 5,6

Answer	
Document Name	

Comment

Constellation aligns with Exelon Corporation and EEI responses to this question

Kimberly Turco 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

There was an assertion made that a linkage exists between the lack of a “material change” in the number of reported incidents and the current CIP-008 language. No compelling evidence was offered to draw the conclusion that the definition of attempts to compromise has a direct relation the number of reported events. It could be that the lack of reportable events is primarily explained by the architecture of protected environments. Many ESPs and EACMS are not exposed directly to the Internet, and so in many cases a compromise or attempt to compromise would necessitate an initial compromise of a corporate environment or bastion host. That higher technical bar, combined with a relatively smaller pool of threat actors with specific interest in accessing protected environments, may be why an increase in reports has not been observed.

Likes 0	
Dislikes 0	

Response

Roger Fradenburgh - Network + Security Technologies - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

NST believes this SAR is attempting to solve a problem that may or may not actually exist, using an approach that risks turning CIP-008 compliance into an unproductive paper chase. The SAR's "Purpose or Goal" section makes the assertion that CIP-008 implementations allowing for subjective determinations of attempt(s) to compromise are the result of a gaps in the Standard that should be remedied. This is itself a subjective judgment and is, in NST’s opinion, most likely a consequence of confirmation bias on the part of the SAR’s authors. Quoting from the SAR, “Since the effective date of CIP-008-6 there has not been a material change in the number of Reportable Cyber Security Incidents or Cyber Security Incidents that were determined to be an attempt to compromise an applicable system.” NST believes this statement makes it clear NERC expected there would be a possibly significant increase in the number of incident reports filed with the E-ISAC and the NCCIC. When this didn’t happen, NERC initiated the “CIP-008-6 Effectiveness Study.” The report authors, clearly convinced this lack of “a material change” is a problem and evidently predisposed to determine the root cause must be flaws in Responsible Entity incident analysis and response procedures and/or in CIP-008-6 itself, decided the culprit is a gap in CIP-008 that allows Entity response teams to make subjective judgments about whether or not one or more cyber events represent “attempts to compromise.” NST has not seen the full report – only a summary released on June 27, 2022 – so we must acknowledge the possibility it contains quantitative data supporting this seemingly arbitrary conclusion. However, absent additional and more compelling information, we oppose the establishment of a Standard Drafting Team to modify CIP-008-6 in the manner the SAR proposes.

Likes 0	
Dislikes 0	

Response

Alison MacKellar - Constellation - 5,6

Answer	
Document Name	
Comment	
Constellation aligns with Exelon Corporation and EEI responses to this question Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	