Comment Report

Project Name:	2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | CIP-008-6
Comment Period Start Date:	10/3/2018
Comment Period End Date:	10/22/2018
Associated Ballots:	2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 IN 1 ST

There were 86 sets of responses, including comments from approximately 176 different people from approximately 116 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The Standard Drafting Team (SDT) created a new definition and modified existing definitions to address the directive in FERC Order No. 848 paragraph 31 regarding "attempts to compromise" without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use existing *Glossary of Terms Used in NERC Reliability Standards* (NERC Glossary) definitions. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident, and the proposed new definition of, Reportable Attempted Cyber Security Incident? If not, please provide comments and alternate language, if possible.

2. The SDT added Electronic Access Control or Monitoring System (EACMS) to applicable systems as opposed to modifying the NERC Glossary EACMS definition to ensure the FERC Order No. 848 paragraph 54 directive to expand reporting requirements to EACMS was met without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use the existing EACMS NERC Glossary definition. Do you agree with the addition of EACMS to the applicable systems column in the tables in CIP-008-6? If not, please provide comments and an alternate approach to addressing the directive, if possible.

3. Do you agree with reporting timeframes included Requirement R4? If you disagree please explain and provide alternative language and rationale for how it meets the directives in FERC Order No. 848.

4. The SDT created Attachment 1 to be used for consistent reporting and intentionally aligned the content with FERC Order No. 848 paragraphs 69 and 73. Do you agree with the content and use of Attachment 1?

5. Do you agree with the required methods of notification proposed by the SDT in Requirement R4, Part 4.2? If no, please explain and provide comments.

6. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R4? If no, please explain and provide comments.

7. Do you agree with the 12-month Implementation Plan? If you think an alternate, shorter, or longer implementation time period is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

8. The SDT proposes that the modifications in CIP-008-6 provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

9. Provide any additional comments for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
BC Hydro and Power Authority	Adrian Andreoiu	1	WECC	BC Hydro	Hootan Jarollahi	BC Hydro and Power Authority	3	WECC
					Helen Hamilton Harding	BC Hydro and Power Authority	5	WECC
Brandon McCormick	Brandon McCormick		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach Utilities Commission	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Javier Cisneros	Fort Pierce Utilities Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steven Lancaster	Beaches Energy Services	3	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	3	FRCC
Luminant Mining Company LLC	Brenda Hampton	7		Luminant	Brenda Hampton	Luminant - Luminant Energy	6	Texas RE
					Stewart Rake	Luminant Mining Company LLC	7	Texas RE
					Alshare Hughes	Luminant - Luminant	5	Texas RE

						Generation Company LLC		
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Kurtz, Bryan G.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Exelon	Chris Scanlon	1		Exelon Utilities	Chris Scanlon	BGE, ComEd, PECO TO's	1	RF
					John Bee	BGE, ComEd, PECO LSE's	3	RF
Santee Cooper	Chris Wagner	1		Santee Cooper	Rene' Free	Santee Cooper	1,3,5,6	SERC
					Rodger Blakely	Santee Cooper	1,3,5,6	SERC
					Bob Rhett	Santee Cooper	1,3,5,6	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
MRO	Dana Klem	1,2,3,4,5,6	MRO	MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administration	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO

					Brad Parret	Minnesota Powert	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service Corporation	3,5,6	MRO
					Jeremy Voll	Basin Electric Power Cooperative	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent ISO	2	MRO
PPL - Louisville Gas and Electric Co.	Devin Shines	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Charles Freibert	PPL - Louisville Gas and Electric Co.	3	SERC
					JULIE HOSTRANDER	PPL - Louisville Gas and Electric Co.	5	SERC
					Linn Oelker	PPL - Louisville Gas and Electric Co.	6	SERC
Seattle City Light	Ginette Lacasse	1,3,4,5	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC

					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
FirstEnergy - FirstEnergy Corporation	Julie Severino	1		FirstEnergy	Aubrey Short	FirstEnergy - FirstEnergy Corporation	4	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Southwest Power Pool, Inc. (RTO)	Kimberly Van Brimer	2	MRO	SPP CIP-008	Matt Harward	Southwest Power Pool (RTO)	2	MRO
					Louis Guidry	Cleco	1,3,5,6	SERC
Manitoba Hydro	Mike Smith	1		Manitoba Hydro	Yuguang Xiao	Manitoba Hydro	5	MRO
					Karim Abdel-Hadi	Manitoba Hydro	3	MRO
					Blair Mukanik	Manitoba Hydro	6	MRO
					Mike Smith	Manitoba Hydro	1	MRO
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC

Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
PSEG	Sean Cavote	1,3,5,6	FRCC,NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	NPCC
					Karla Barton	PSEG - PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co.	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co.	1	RF
Associated Electric Cooperative, Inc.	Todd Bennett	1,3,5,6		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC

					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	NPCC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					Ryan Ziegler	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC

1. The Standard Drafting Team (SDT) created a new definition and modified existing definitions to address the directive in FERC Order No. 848 paragraph 31 regarding "attempts to compromise" without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use existing *Glossary of Terms Used in NERC Reliability Standards* (NERC Glossary) definitions. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident, and the proposed new definition of, Reportable Attempted Cyber Security Incident? If not, please provide comments and alternate language, if possible.

Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6

Answer	Yes
Document Name	

Comment

Does not limit what must be reported, but Entity will need to devote significant resources, which takes away time from addressing cyber attacks

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

PPL NERC Registered Affiliates generally agree with the changes. However, neither the modified term "Reportable Cyber Security Incident" nor the new term "Attempted Cyber Security Incident" appears to include compromise or disruptions of a Cyber Asset supporting a PACS. Specifically, EACMS and ESP are mentioned, but a PSP is not.

This omission of Cyber Assets supporting a PACS, if purposeful, seems inconsistent with other NERC guidance. We would suggest either providing clear rationale for this omission or correcting the language for consistency if it was not left out on purpose.

Likes 0	
Dislikes 0	

Response

Kelsi Rigby - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	Revisions to Defined Terms.docx

Comment

AZPS recommends that the proposed definitions be reviewed to ensure there is not redundancy of terms within other defined terms as such redundancy can result in unintended consequences. For example, the term Cyber Security Incident references attempts to compromise. Thus, the incorporation of the same or similar verbiage into the newly proposed term Reportable Attempted Cyber Security Incident is not necessary. Accordingly, APS proposes the revisions to the defined terms Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident shown in the attached.

Likes 0	
Dislikes 0	

Response

Douglas Johnson - American Transmission Company, LLC - 1

Answer	Yes
Document Name	

Comment

American Transmission Company LLC (ATC) supports the proposed new and modified definitions; however, believes there may be opportunity for further improvement. ATC offers the following perspective and rationale and requests the SDT consider this as an alternative approach:

The existence of the Physical Security Perimeters (PSPs) within the Cyber Security Incident definition causes confusion within the Requirements. To gain ultimate clarity, ATC requests the SDT remove PSP from the Cyber Security Incident definition and consider the creation of a second new definition to assure Registered Entity's Cyber Security Incident Planning and Response Programs continue to take into account a Cyber Security breach that may occur through physical means. ATC offers the proposed draft definition language as originally directed by FERC in Order 706 paragraph 656:

Potential Cyber Security Incident (new definition):

A malicious physical act or suspicious physical event that:

- Compromises, or was an attempt to compromise the Physical Security Perimeter or;
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Cyber Security Incident (adjustments to proposed modified definition):

A malicious act or suspicious event that:

- Has been determined to be a Potential Cyber Security Incident
- Compromises, or was an attempt to compromise the Electronic Security Perimeter or Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

ATC asserts this approach:

1. May help simplify and clarify the scope of the Definitions, Requirement language, and Attachment 1,

2. Remove the ambiguity that a physical act/event alone constitutes a cyber act/event; thereby removing the opportunity for interpretative debate of what could be 'perceived' or 'implied' as reportable under CIP-008. This helps clarify that physical acts/events involving a PSP are to be treated as cyber 'potentialities'.

3. Draws a clearer tie between CIP-006 and CIP-008 while adding clarity to the relationship between physical acts/events that may manifest into cyber acts/events,

4. Retains the obligation for Registered Entities to investigate physical acts/events as potential attack vectors for Cyber Security Incidents that, once determined, must trigger Cyber Security Incident Response,

5. Achieves the current and historical FERC directives, and

6. Does not change the intention nor results of Cyber Security Incident planning and response.

Next, to complete this concept, the Requirement language could be modified as follows:

A. Add 'BES" in front of "Cyber Security Incident Response plan(s)" in CIP-008-6 Requirement R1 to draw a clear tie to CIP-006-6 Requirement R1 Parts 1.5, 1.7, and 1.10 without having to open CIP-006 for modifications. Proposal:

R1. Each Responsible Entity shall document one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

B. Add the explicit obligation to investigate Potential Cyber Security Incidents to Requirement R1 Part 1.1. Proposal:

One or more processes to:

1. Investigate Potential Cyber Security Incidents, and

2. Identify, classify, and respond to Cyber Security Incidents.

C. Remove the confusing PSP exclusion from Requirement R4 Part 4.1. Proposal:

Initial notifications and updates for Reportable Cyber Security Incidents and/or Reportable Attempted Cyber Security Incidents shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;
2. The attack vector used; and
3. The level of intrusion that was achieved or attempted.

D. Simplify CIP-008-6 Attachment 2, by removing the 'Note' about PSP(s) from Section: Incident Type, Field Name: Reportable Attempted Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Under # 3 in the proposed modification of terms, The term Electronic Access control of monitoring should read Electronic Access control or monitoring systems. We think the definition to be overly broad, determining what is an “attempt” or “suspicious” is not defined entities will not apply the definition consistently. The SDT should consider including PACS. Should not include physical security perimeter because it is inconsistent with the definition to only include cyber incidents.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Propose adding ‘as determined by the entity’ to the definition.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

WECC voted yes to approve the revisions to CIP-008 but is providing comments for consideration that WECC believes would improve the Standard.

The “Cyber Security Incident” Definition needs to be revised to, "*[…] (3) Electronic Access Control **OR** Monitoring System for High or Medium Impact BES Cyber Systems, […]"* rather than "*Control OF Monitoring."*

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

NRG requests that NERC consider providing additional clarity in definition of Reportable Cyber Security Incident to further specify "attempt" meaning in the "Reportable Attempted" term (for example, intentional attempt) within the glossary of terms (NERC) or within the technical guidance of the draft standard changes relating to CIP-008-6.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI

Answer	
Document Name	

Comment
AECI supports the comments provided by NRECA.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment
The proposed revised definitions of Reportable Attempted Cyber Security Incident and Reportable Cyber Security incident appear to expand on the definition of EACMS. The both include the following language: "*Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting*." Texas RE recommends that it would be cleaner to include these functions in the definition of EACMS. In the proposed definition of Reportable Attempted Cyber Security Incident, the phrase "*attempt to compromise or disrupt*" is very broad. Texas RE recommends describing in detail what this means. Texas RE is concerned the proposed language may allow for entities not reporting threats to Physical Security Perimeters (PSP). First, the proposed definition of Cyber Security Incident includes the PSP. The proposed definition of Reportable Cyber Security Incident does not include PSP. Additionally, Part 4.1 includes the language, "*Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter*". A compromised Physical Security Perimeter could be just as damaging as a compromised Electronic Security Perimeter. Texas RE recommends the definition of Reportable Cyber Security Incident and Part 4.1 apply to PSPs as well.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant

Answer	
Document Name	

Comment

Luminant does not agree with the proposed definition for Reportable Attempted Cyber Security Incident. As currently written there are no boundaries on what constitutes an “attempt” which will lead to different interpretations and therefore inconsistent enforcement. For example, would malware present on a Transient Cyber Asset that is detected during a scan of that asset be considered an attempt to compromise or disrupt reliability tasks, an ESP or EACMS? At its very core, all malware is an attempt to compromise something, but the majority of malware is not at all targeted toward disrupting power operations. Another example is extensive scanning to identify weaknesses and gather any available information. While this is often the first step of an actual attack, it is also often not targeted or performed by inexperienced actors. While such activities should be noted and investigated, in and of themselves they are generally not treated as actual or attempted cyber security incidents.

Luminant recommends the SDT clarify the intent of this reporting. If the focus is to establish a more extensive baseline understanding of the nature of cyber security threats and vulnerabilities encountered within the industry than perhaps we can create a treatment similar to aggregate self-logging for “minimum risk” events that require periodic reporting. The examples above would be included in such reporting. This approach could reduce the debate over what constitutes an “attempt” and an entity can be considered in compliance as long as the event is reported. Much like aggregate self-logging, if the ERO disagrees that an activity is “minimum risk,” they can address that individually and disseminate lessons learned to evolve the definition. In this approach, an event that has clear indicators of intent to disrupt reliability tasks, ESPs, PSPs, EACMS or BCS would not be eligible for aggregate reporting and would instead follow a more rigorous approach.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

APPA appreciates the drafting team working to address FERC’s directives while preserving the integrity CIP-003’s scope and CIP standards that use the NERC Glossary definitions. However, public power does not agree with the proposed definition for Reportable Attempted Cyber Security Incident and offers an alternative below.

APPA’s concern with the proposed definition is due to the use of, “one or more reliability tasks of a functional entity.” The use of the term Reportable Attempted Cyber Security Incident and that proposed definition, introduce ambiguity to determining attacker intent, making it difficult to determine if an attacker intended to compromise or disrupt one or more reliability tasks.
For example, in the event of a ransomware attack affecting an EMS workstation – it would be difficult to distinguish if this was an attempt to compromise or disrupt a reliability task, or if the attacker was interested in financial gain? The following definition attempts to eliminate this type of concern:

Reportable Attempted Cyber Security Incident:
A Cyber Security Incident that was an attempt to compromise or disrupt:
• the operation of a BES Cyber System; or
• Electronic Security Perimeter; or
• Electronic Access Control or Monitoring System (EACMS) that provide any of the

following functions: (1) authentication; (2) monitoring and logging; (3) access control;
(4) Interactive Remote Access; or (5) alerting.

Additionally, the phrase “attempt to compromise or disrupt” introduces ambiguity in itself, unless defined to include all access attempts. What constitutes an attempt to compromise or disrupt? Would a port scan be an attempt to compromise or disrupt? Would 5 failed login attempts within a specified timeframe reach that threshold?

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	
Document Name	

Comment

The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT has joined the comments of the ISO/RTO Council and offers these supplemental comments.

Regarding the “Cyber Security Incident” definition, “High or Medium Impact BES Cyber Systems” is not necessary in the definition. EACMSs are already limited to High and Medium Impact BES Cyber Systems. Also, the applicability is addressed in the Applicable Systems column of the table with each requirement.

Regarding the definition of “Reportable Cyber Security Incident,” the details of the EACMS functions are not necessary; including the list of functions may have the unintended consequence of excluding things that should be included.

Regarding the definition of “Reportable Attempted Cyber Security Incident,” ERCOT questions the need for this definition. The reporting timelines can be addressed with the requirement parts for compromise vs. attempt to compromise.

Regarding the concept of “attempt”generally, ERCOT requests more specificity and clarification on the types and thresholds of attempts that are expected to be reported. As FERC Order 848 recognized, specificity in the reporting threshold is needed “to ensure that [the reporting obligation] would provide meaningful data without overburdening entities.” FERC Order 848 at ¶ 52 (quoting NERC comments). Lack of specificity will result in differing

interpretations of “attempt” across the industry. A conservative reading of this term could yield substantial over-reporting of activities that do not bear any indication of malicious intent or harm. This could lead to over-reporting of incidents to E-ISAC and ICS-CERT, thereby reducing visibility of reports of legitimate incidents. Other entities may interpret the term in such a way that leads to information regarding important events not being reported. To avoid these results, ERCOT strongly encourages the SDT to identify specific reporting thresholds such as those proposed by the ISO/RTO Council.

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The phrase “attempts to compromise” is overly broad. The intent of the scope of this clause should to be more clearly defined as the undefined term could be interpreted in many different ways . Additionally, while we agree with the five criteria proposed, additional criteria for the reporting of an attempted compromise should also be included to address the bounds of attempts.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

How do we measure an attemps to compromise?

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

Definitions should not include EACMs. Every packet denied by a firewall would generate a potential Reportable Attempted Cyber Security Incident, making this requirement onerous for the entities.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The definition of “Reportable Attempted Cyber Security Incident” is still unclear. What does it mean to attempt? What includes an attempt?

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

Reportable Attempted Cyber Security Incident and Cyber Security Incident have defined inconsistencies such as one references BES operation and the other for Reliability tasks. Reportable Attempted Cyber Security Incident uses "attempt" in the definition and never defines what is an "attempt".	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The proposed new term Reportable Attempted Cyber Security Incident is defined using the proposed modified term Cyber Security Event. This redundancy suggests that, instead of creating a new term, the definition of Cyber Security Incident should be expanded to include the desired elements of the proposed new term.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
The proposed new term Reportable Attempted Cyber Security Incident is defined using the proposed modified term Cyber Security Event. This redundancy suggests that, instead of creating a new term, the definition of Cyber Security Incident should be expanded to include the desired elements of the proposed new term.	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	

Comment
Platte River is okay with the draft requirement language as proposed in CIP-008-6. Platte River is recommending a modification be made to the proposed new term: Reportable Attempted Cyber Security Incident. The proposed term assumes the Responsible Entity can determine the intent of the individual whose activity was identified. Since, by definition, the attempt was unsuccessful, the Registered Entity cannot know what the individual was trying to accomplish. The method to implement the definition, as proposed, is not clear. Platte River is recommending the following modifications be made to the definition: Reportable Attempted Cyber Security Incident: A Cyber Security Incident that was an attempt to circumvent: · Electronic Security Perimeter; or · Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting Platte River believes this definition better captures the intent of the changes in CIP-008-6. Registered Entity staff are better able to determine if the individual was attempting to circumvent their security controls without having to determine the individual's intent.

Likes 0	
Dislikes 0	

Response

Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	No
Document Name	

Comment
The proposed new term Reportable Attempted Cyber Security Incident is defined using the proposed modified term Cyber Security Event. This redundancy suggests that, instead of creating a new term, the definition of Cyber Securtiy Incident shoudl be expanded to include the desired elements of the proposed new term.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	
Comment	

The proposed definition of “Reportable Attempted Cyber Security Incident” does not provide enough specificity to make a determination as to whether an incident was attempted. Lack of clarity in this definition would make the difference between TVA reporting: 1) only those incidents that had a high potential of success but were not successful; and 2) any and all efforts to gain intelligence about NERC CIP scoped systems. The subsequent reporting of the latter could be overwhelming to TVA, E-ISAC, and ICS-CERT.

In addition, lack of specificity in the definition of the word “disrupt” could have a similar effect. This term should be limited to disruptions from cyber events to avoid reporting of purposeful disruptions (e.g., asset reboots for maintenance purposes). Without this, all maintenance disruptions could be reportable.

Likes 0	
Dislikes 0	
Response	

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	
Comment	

The Cyber Security Incident definition is rooted in the law (Section 215) definition: “The term ‘cybersecurity incident’ means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system.” This definition clearly identifies the target of the event to be “programmable electronic devices and communication networks.” The current NERC glossary term includes PSPs as a target. PSPs are not “programmable electronic devices and communication networks.” The definition would be better aligned with the law by deleting “Physical Security Perimeter’ from the Cyber Security Incident definition. “Programmable electronic devices and communication networks” create the concept of ESPs or are EACMS. So references in the definition to ESPs and EACMS don’t contradict the law (Section 215).

With the addition of Reportable Attempted Cyber Security Incident, the existing term Reportable Cyber Security Incident should be revised to more clearly delineate the difference between the two terms. For example: Reportable Successful Cyber Security Incident or Reportable Actual Cyber Security Incident. We recognize this would require minor changes in CIP-003. In the webinar, there was also mention of tracking historical metrics with future metrics. It shouldn’t be difficult to add historical metrics to the future metrics especially given there were so few historical metrics. These two items are worth it to minimize confusion.

Likes 0	
Dislikes 0	
Response	

larry brusseau - Corn Belt Power Cooperative - 1

Answer	No

Document Name	

Comment

The definition of a Cyber Security Incident includes compromise or attempted compromise of a Physical Security Perimeter (PSP), but in Part 4.1 the report for PSP's are excluded. If the intent is to only report on incidents that actually compromise cyber equipment then the standard would be clearer if the PSP was removed from the Cyber Security Incident definition as shown below.

Change Cyber Security Incident definition to read: A malicious act or suspicious event that:

{C}· Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter or (2) Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;

{C}· Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Change Part 4.1 to read: Reportable Cyber Security Incident initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted

For example, if a PSP was breached and no BES Cyber Systems were compromised then there was not actually a Cyber Security Incident. The breach may have been due to theft or vandalism not involving BES Cyber Systems.

Additionally, the **attempt to compromise** definition needs to be consistent with the current version of the standard, CIP-008-5 R1.1, which requires each entity to have a process to identify if a malicious act or suspicious event was an attempt to compromise the Electronic Security Perimeter.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA appreciates the challenge facing the SDT in addressing the directive regarding "attempts to compromise" as required by FERC Order No. 848. BPA recommends the SDT revise CIP-008-6 to include clear language allowing the entity to define "an attempt." This will take into consideration entities of varying size facing differing threat vectors.

Likes 0	
Dislikes 0	

Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
The Reportable Attempted Cyber Security Incident definition as written and interpreted by the SDT is intended to provide entities flexibility to define “attempt” and a process around reporting. This may result in a very low threshold that is defined by entities and result in underreporting with no added value. On the flip side, this can also result in unnecessary overload if reporting criteria is set too high. Another concern is that this flexibility also allows for an auditor’s own interpretation of “attempt”. BC Hydro does not see any value-add in making reportable attempts a mandatory requirement as opposed to having this be a voluntary process.	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	No
Document Name	
Comment	
Physical Security Perimeter (PSP) should be removed from the Cyber Security Incident definition. It is not consistent with the proposed revised Reportable Cyber Security Incident and the proposed new term Reportable Attempted Cyber Security Incident. If the intent is to keep PSP then this should be represented in a new PSP specific definition.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The definition of a Cyber Security Incident includes compromise or attempted compromise of a Physical Security Perimeter (PSP), but in Part 4.1 the report for PSP's are excluded. If the intent is to only report on incidents that actually compromise cyber equipment then the standard would be clearer if the PSP was removed from the Cyber Security Incident definition as shown below.

Change Cyber Security Incident definition to read: A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter or (2) Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Change Part 4.1 to read: Reportable Cyber Security Incident initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted

For example, if a PSP was breached and no BES Cyber Systems were compromised then there was not actually a Cyber Security Incident. The breach may have been due to theft or vandalism not involving BES Cyber Systems.

Additionally, the **attempt to compromise** definition needs to be consistent with the current version of the standard, CIP-008-5 R1.1, which requires each entity to have a process to identify if a malicious act or suspicious event was an attempt to compromise the Electronic Security Perimeter.

Likes 1	Central Hudson Gas & Electric Corp., 1, Pace Frank
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	No
Document Name	

Comment

WEC Energy Group agrees that the new and modified definitions meet FERC's directive in Oder No. 848 and we generally support these definitions except for one term. WEC Energy Group is concerned that the term "attempt to compromise" is ambiguous and insufficiently understood.

The Commission used the term "attempt to compromise" in Order 848 but also stated that the directive was "to augment the reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm reliable operation of the BES." (see P2) We believe this was meant to focus the reporting on incidents that represent a clear threat to the BES.

We believe the SDT should consider either defining the term or developing boundaries that can be consistently applied by the industry to provide clearer focus on incidents that have been identified as genuine threats to protected BES Cyber Systems. This would better ensure the term is understood broadly by industry allowing entities to develop measured and consistent processes that ensure new requirements do not interfere or otherwise complicate industry efforts to identify issues that represent serious risks to BES Reliability.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

Given that the definition of Cyber Security Incident includes “compromise or was an attempt to compromise”, the definitions of the modified Reportable Cyber Security Incident and the new Reportable Attempted Cyber Security Incident are broad enough to bring almost each Cyber Security Incident to become a reportable one. We disagree that each compromise or was an attempt to compromise of ESP or EACMS needs to be reported unless it affects reliability, in that it may result in millions of reports per year. If it is intended to include attempts of compromise affecting reliability to be reportable, we suggest only to revise the existing Reportable Cyber Security Incident definition rather than creating additional reportable one: “Reportable Cyber Security Incident: A Cyber Security Incident that has compromised or disrupted or was an attempt to compromise or disrupt one or more reliability tasks of a functional entity.”

Likes 0	
Dislikes 0	

Response

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	

Comment

As drafted, it is difficult to discern a difference between the definitions for *Reportable Cyber Security Incident* and *Reportable Attempted Cyber Security Incident*. Additionally, we do not think it is reasonable or necessary to report all "knocks on the door" to our ESPs or EACMS. We propose the following modifications (or something similar) to both defitions so that there is a more clear distinction between the two and clear reporting expectations.

Reportable Cyber Security Incident:

A Cyber Security Incident that has disrupted

- One or more reliability task of a functional entity; or
- BES Cyber System; or
- Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.

Reportable Attempted Cyber Secuirty Incident:

A Cyber Security Incident where there was access into an ESP, or an EACMS, but there was no resulting disruption to the EACMS, BES Cyber System, or a reliability task.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

SCL believes that by modifying the definition of Cyber Security Incident, the intent of the FERC order can be met. The definition of Reportable Attempted Cyber Security Incident is not necessary if these changes are made.

Likes 0	
Dislikes 0	

Response

Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy

Answer	No
Document Name	

Comment

The definition of Reportable Attempted Cyber Security Incident is circular with Cyber Security Incident. The term *Cyber Security Incident* already included the term “attempt” in a different meaning.

Suggested updated definitions:

Cyber Security Incident:

A malicious or suspicious event related to:

- an Electronic Security Perimeter or
- a Physical Security Perimeter or
- Electronic Access Control or Monitoring System for High and Medium Impact BES Cyber Systems

Reportable Cyber Security Incident:

A Cyber Security Incident that successfully compromised or disrupted:

- one or more reliability tasks of a functional entity or
- an Electronic Security Perimeter or
- an Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that attempted to compromise or disrupt:

- one or more reliability tasks of a functional entity or
- an Electronic Security Perimeter or
- an Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.

Attempted should also be defined to provide the appropriate guidance as to what constitutes a Reportable Attemped Cyber Security Incident. Some possible items to include as an attempt are:

- was directed specifically at or appeared to be specifically directed at an ESP, ECASM or BCA
- was not incidental to other network activity, including bulk, non-specific undesired network activity

could have feasibly compromised an ESP, EACMS or BCA by its very nature

Likes 0	
Dislikes 0	

Response

Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC

Answer	No
Document Name	

Comment

The definition of a Cyber Security Incident includes compromise or attempted compromise of a Physical Security Perimeter (PSP), but in Part 4.1 the report for PSP's are excluded. If the intent is to only report on incidents that actually compromise cyber equipment then the standard would be clearer if the PSP was removed from the Cyber Security Incident definition as shown below.

Change Cyber Security Incident definition to read: A malicious act or suspicious event that:

• Compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter or (2) Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;

• Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system.

Change Part 4.1 to read: Reportable Cyber Security Incident initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted

For example, if a PSP was breached and no BES Cyber Systems were compromised then there was not actually a Cyber Security Incident. The breach may have been due to theft or vandalism not involving BES Cyber Systems.

Additionally, the **attempt to compromise** definition needs to be consistent with the current version of the standard, CIP-008-5 R1.1, which requires each entity to have a process to identify if a malicious act or suspicious event was an attempt to compromise the Electronic Security Perimeter.

ALSO:

Reclamation recommends the definition for Reportable Attempted Cyber Security Incident be expanded to include disruption or attempted compromise of Physical Security Perimeters and Physical Access Control Systems. This would allow identifying a Facility as a potential target without its reliability or operations being affected.

Reclamation also recommends removing the following language from the bullet point for EACMS because it is redundant of the EACMS definition: *"that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting."*

Therefore, Reclamation recommends the proposed new term be changed

from:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:

One or more reliability tasks of a functional entity; or

Electronic Security Perimeter; or

Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

to:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:

One or more reliability tasks of a functional entity; or

Electronic Security Perimeter (ESP); or

Physical Security Perimeter, including locally-mounted hardware or devices; or

Physical Access Control Systems (PACS); or

Electronic Access Control or Monitoring System (EACMS).

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 6

Answer	No
Document Name	

Comment

"attempted" is to broad of a term. Our SMEs have concerns that the term could be viewed to broadly which could then in turn result in altert fatique and credible indicents could then be missed.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3

Answer	No
Document Name	

Comment

The phrase ". . . an attempt to . . ." in the proposed modification of the term Cyber Security Incident and in the proposed new term Reportable Cyber Security Incident is too vague. Modification of the phrase ". . . an attempt to . . ." to ". . . an attempt, which, if successful, would have resulted in the compromise or disruption . . ." or something similar seems to be closer to the intent of the proposed changes.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Due to a lack of published draft Implementation Guidance, it is challenging to fully assess the impacts of the new “Reportable Attempted Cyber Security Incident” definition and the addition of EACMS in terms of how much additional investigation and reporting volume will fall on the Responsible Entity. Providing specific guidance with examples of what would and would not be a “Reportable Attempted Cyber Security Incident” may alleviate these concerns.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Agree with the language of the definition, but believe that the addition of a new definition so closely related and worded to two existing definitions could cause confusion among industry. Would suggest revisiting the topic as a SDT.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

NRECA is concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, NRECA believes that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team’s approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. NRECA urges the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Utility Services agrees with APPA's comments. Additionally, we note that the definition of Reportable Attempted Cyber Security Incident (as well as that of Reportable Cyber Security Incident) not including a Cyber Security Incident to a Physical Security Perimeter that does not compromise or disrupt one of the three bulleted items, and wonder if that was an intentional decision.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We are concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, we believe that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team's approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. We urge the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	No
Document Name	
Comment	

- Overall our SMEs believe this standard should focus more on the risk and benefits of monitoring events within the power grid versus work, effort and expense of collecting data on potential cyber intrusions.Second bullet fails to capture the "… for High or Medium Impact BES Cyber Systems…"Proposed Modified Term, "Reportable Cyber Security Incident" - None of the listed bullets currently capture Physical attacks or compromises of the physical perimeter.Recommend deleting the term "Reportable Attempted Cyber Security Incident" and modifying the definition of Reportable Cyber Security Incident to include the following: A Cyber Security Incident that has compromised, disrupted or was an attempt to compromise or disrupt
- Also agree with NPCC submitted comments

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

I support all comments submitted by Terry Harbour, Berkshire Hathaway Energy-MidAmerican Energy Company.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Definitions do not limit what must be reported. Entity will need to devote significant resources to reporting – which takes away resources from addressing cyber attacks

Some concern with "Reportable Cyber Security Incident" for field locations (substations & generators) since these locations have fewer defense layers.

Concerns that the "Cyber Security Incident" puts the burden of determining intent – is the intent to "compromise" or "disrupt." Expect this lack of clarity to result in in over-reporting which makes finding the real incident akin to a needle in the haystack.

Likes 0	
Dislikes 0	

Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	No
Document Name	
Comment	
GSOC is concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, GSOC believes that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team's approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. GSOC urges the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	
Comment	
See comments from the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	

Proposed modified terms and Proposed new term include a separate definition for EACMS when compared to the current EACMS definition in the NERC Glossary. The proposed modifications and proposed new term should reference the existing definition of EACMS. There should be no difference in identifying EACMS for incident reporting purposes vs systems already identified as EACMS.

Proposed modified terms and Proposed new term include the phrases “attempt to compromise” and “attempt to disrupt”. Further clarification is needed for the meaning of these phrases to guide Responsible Entities on reporting requirements.

Likes 0	
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

Vectren agrees with the modified definitions of Cyber Security Incident and Reportable Cyber Security Incident. However, the new definition of Reportable Attempted Cyber Security Incident is very broad which leaves it open to interpretation. This definition as written will cause an unreasonable administrative burden on the entity, requiring us to dedicate significant time and resources to track and investigate potential attempts.

By investigating blocked attempts, the focus is shifted away from higher risks. The resources of E-ISAC and ICS-CERT will also be impacted by a larger volume of reports regarding lower risk threats including the potential attempts to compromise. Ultimately, this shift in focus could lead to a compromise of safety and reliability of the BES.

Recognizing the task of the SDT to draft a reasonable definition, the definition in its present form will not serve the intent of the FERC Order No. 848 directive. We would suggest the SDT narrow the scope of “attempts to compromise” within the definition to alleviate the potential burden to the entity, E-ISAC and ICS-CERT.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

The proposed modification to the definition of Reportable Cyber Security Incident indirectly alters and expands the current definition of Electronic Access Control or Monitoring System (EACMS), potentially bringing into scope Cyber Assets for CIP-008 reporting that Responsible Entities had not previously determined in scope for CIP overall. CenterPoint Energy Houston Electric, LLC (CenterPoint Energy) proposes that the language following

the listing of EACMS in the Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident definitions, "*that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting"* be removed.

For the proposed new term of Reportable Attempted Cyber Security Incident, the determination of intent in the phrase "attempt to compromise or disrupt" is subjective and therefore difficult to apply as a standard. Any packet or connection rejected by a firewall, access control list, or logged access attempt could be interpreted as existing security controls working as designed or as an attempted compromise to possibly report. This could be millions of attempts, per day, per EACMS under normal operations. No Technical Rationale or Implementation Guidance is offered to assist with characterization of an attempt to compromise or compromise of an EACMS. CenterPoint Energy acknowledges the Technical Rationale and Justification provided by the SDT and the ongoing efforts to update the Guidelines and Technical Basis of the CIP Standards. For the benefit of these modifications, successful ballot, and implementation, CenterPoint Energy suggests that the SDT coordinate with the CIP Guidelines and Technical Basis Review team to provide the revised guidance with this project's materials or adjust the Implementation Plan to allow for the development of the guidance well in advance of the effective date. Most notably, the guidance should assist with characterization of an attempt to compromise or compromise of an EACMS.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy recommends that further clarification be given on what constitutes an actual "attempt" when determining whether a Reportable Attempted Cyber Security Incident has occurred. Perhaps this could be made clearer in an Implementation Guide with examples of what an "attempt" should be considered as.

Likes 1	Long Island Power Authority, 1, Ganley Robert
Dislikes 0	

Response

Steven Sconce - EDF Renewable Energy - 5

Answer	No
Document Name	

Comment

More guidance is needed regarding the definition of what constitutes an "attempt."

Likes 0	
Dislikes 0	

Response
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	

Comment
FMPA agrees with the below comments from APPA: : APPA appreciates the drafting team working to address FERC's directives while preserving the integrity CIP-003's scope and CIP standards that use the NERC Glossary definitions. However, public power does not agree with the proposed definition for Reportable Attempted Cyber Security Incident and offers an alternative below. APPA's concern with the proposed definition is due to the use of, "one or more reliability tasks of a functional entity." The use of the term Reportable Attempted Cyber Security Incident and that proposed definition, introduce ambiguity to determining attacker intent, making it difficult to determine if an attacker intended to compromise or disrupt one or more reliability tasks. For example, in the event of a ransomware attack affecting an EMS workstation – it would be difficult to distinguish if this was an attempt to compromise or disrupt a reliability task, or if the attacker was interested in financial gain? The following definition attempts to eliminate this type of concern: **Reportable Attempted Cyber Security Incident:** A Cyber Security Incident that was an attempt to compromise or disrupt: · the operation of a BES Cyber System; or · Electronic Security Perimeter; or · Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting. Additionally, the phrase "attempt to compromise or disrupt" introduces ambiguity in itself, unless defined to include all access attempts. What constitutes an attempt to compromise or disrupt? Would a port scan be an attempt to compromise or disrupt? Would 5 failed login attempts within a specified timeframe reach that threshold?

Likes 0	
Dislikes 0	

Response
Jodirah Green - ACES Power Marketing - 6

Answer	No
Document Name	
Comment	

Attempts to compromise are a constant in an interconnected world. Expanding the criteria of Reportable Incidents will be burdensome to entities and NERC without considerable benefit. The CIP standards and the protections required within are what reduce cybersecurity risk and prevent attempts to compromise. Any unsuccessful attempts are a sign the controls are working and are not incidents, they are cybersecurity events. Where controls fail or are bypassed and or compromised ie an actual incident[1], should be the only Reportable Cybersecurity Incident.

{C}[1]

Likes 0	
Dislikes 0	
Response	

Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns

Answer	No
Document Name	
Comment	

The proposed new term ""Reportable Attempted Cyber Security Incident"" is redundant. Already included within the definition of "Cyber Security Incident" is the statement *"or was an attempt to compromise"*. Therefore the defined term of a "Reportable Cyber Security Incident" is inclusive of this condition. A solution would be to indicate the nature of the reportable event as successful, or attempted.

In addition, ITC concurs with the follwing comments submitted by SPP:

"**Grammatical Issues:** The draft definition for Cyber Security Incident contains a typographical error that should be fixed prior to final ballot. The terms should be "Electronic Access Control or Monitoring System for High or Medium Impact BES Cyber Systems."

Additionally, the definitions of Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident should reference EACMS consistent with the general definition of Cyber Security Incident: "Electronic Access to Control or Monitoring System (EACMS) for High or Medium Impact BES Cyber Systems that provide the following functions…"

Substantive Issues: The proposed definitions of "Cyber Security Incident" and "Reportable Attempted Cyber Security Incident" includes the language "attempt to compromise or disrupt" as an element of the condition. The statement "attempt to compromise or disrupt" is unclear, ambiguous, and should be further defined by criteria. The SSRG supports the following categories proposed by the SWG in its comments:

- If discovered, persistent compromise and attempts to pivot to critical systems could be interpreted as facilitating effort to harm reliable operation.
- Insider incidents involving access to ESP's.
- Incidents involving ICS systems (such as ICCP network or server equipment).

- Incidents involving Physical access that could involve BES Cyber Systems.
- Events and incidents noted as involving ESP's.
- Incidents with progress along a kill chain to the Modify/Install step (reference: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf). "

Does this need to address entity definition of attempt (confirmed attempt?). Does the exclusion of PSP attempts and disruption make sense as far as reporting goes? PSP's would seem to be as important as ESP's in this regard.

With regard to the proposed definition of "Reportable Cyber Security Incident": Should this simply be EACMS without restriction or one of other descriptions of EACMS?

With regard to the proposed definition of "Reportable Attempted Cyber Security Incident": Is this definition needed given the prior definitions (note "attempt" shows up in Cyber Security Incident already)?"

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - 1,3,5 - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI agrees that the new and modified definitions meet FERC's directive in Oder No. 848 and we generally support these definitions except for one term. EEI is concerned that the term "attempt to compromise" is ambiguous and insufficiently understood.

The Commission used the term "attempt to compromise" in Order 848 but also stated that the directive was "to augment the reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm reliable operation of the BES." (see P2) We believe this was meant to focus the reporting on incidents that represent a clear threat to the BES.

We believe the SDT should consider either defining the term or developing boundaries that can be consistently applied by the industry to provide clearer focus on incidents that have been identified as genuine threats to protected BES Cyber Systems. This would better ensure the term is understood broadly by industry allowing entities to develop measured and consistent processes that ensure new requirements do not interfere or otherwise complicate industry efforts to identify issues that represent serious risks to BES Reliability.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No

Document Name	
Comment	
Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
With the addition of Reportable Attempted Cyber Security Incident, the existing term Reportable Cyber Security Incident should be revised to more clearly delineate the difference between the two terms. Actual and attempted compromise of assets including EACMS. The word “attempt’ can be defined differently than what the OE-417. An “attempt” could be reportable if a declared incident could potentially affect our in-scope assets. Each entity has a threshold that depends on the resources and skills that they have. EACMs have attempts every day. We could not find language defining an “attempt to compromise”. The current NERC glossary term includes PSPs as a target. PSPs are not, “programmable electronic devices and communication networks.” The definition would be better aligned with the law by deleting, “Physical Security Perimeter” from the Cyber Security Incident definition. “Programmable electronic devices and communication networks” create the concept of ESPs or are EACMS. So references in the definition to ESPs and EACMS don’t contradict the law (Section 215	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
Proposed modified terms and Proposed new term include a separate definition for EACMS when compared to the current EACMS definition in the NERC Glossary. The proposed modifications and proposed new term should reference the existing definition of EACMS. There should be no difference in identifying EACMS for incident reporting purposes vs systems already identified as EACMS.	

Proposed modified terms and Proposed new term include the phrases “attempt to compromise” and “attempt to disrupt”. Further clarification is needed for the meaning of these phrases to guide Responsible Entities on reporting requirements.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
What constitutes an attempt? Without a clearer definition, the concern is that we will be reporting attempts every day and having continuous follow-up reporting for things that may not necessarily add any additional security. The Standard should provide criteria for attempts and/or make it clear within the requirement that the Entity defines a process to make that determination. If not, it is left open for auditor interpretation and potential violations for not reporting something they think should have been reported.	
Likes 0	
Dislikes 0	
Response	
Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	No
Document Name	
Comment	
Tacoma Power agrees with APPA's comments: "APPA appreciates the drafting team working to address FERC’s directives while preserving the integrity CIP-003’s scope and CIP standards that use the NERC Glossary definitions. However, public power does not agree with the proposed definition for Reportable Attempted Cyber Security Incident and offers an alternative below. APPA’s concern with the proposed definition is due to the use of, “one or more reliability tasks of a functional entity.” The use of the term Reportable Attempted Cyber Security Incident and that proposed definition, introduce ambiguity to determining attacker intent, making it difficult to determine if an attacker intended to compromise or disrupt one or more reliability tasks. For example, in the event of a ransomware attack affecting an EMS workstation – it would be difficult to distinguish if this was an attempt to compromise or disrupt a reliability task, or if the attacker was interested in financial gain? The following definition attempts to eliminate this type of concern: **Reportable Attempted Cyber Security Incident:**	

A Cyber Security Incident that was an attempt to compromise or disrupt:
· the operation of a BES Cyber System; or
· Electronic Security Perimeter; or
· Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.

Additionally, the phrase “attempt to compromise or disrupt” introduces ambiguity in itself, unless defined to include all access attempts. What constitutes an attempt to compromise or disrupt? Would a port scan be an attempt to compromise or disrupt? Would 5 failed login attempts within a specified timeframe reach that threshold?"

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper believes that “Attempted” in Reportable Attempted Cyber Security Incident needs to be defined further. The SDT should provide guidance on what needs to be reported as a Reportable Attempted Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

The phrase “for High or Medium Impact BES Cyber Systems” should be removed from the definition for Cyber Security Incident. Applicability information should be in the Standards and requirement language, not in definitions. Although Low Impact facilities are not required to define an ESP or EACMS, entities that have defined these controls at Low Impact assets should report compromises or attempted compromises to the ESP or EACMS if they detect them.

Likes 0	
Dislikes 0	

Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

Comments: APPA appreciates the drafting team working to address FERC's directives while preserving the integrity CIP-003's scope and CIP standards that use the NERC Glossary definitions. However, public power does not agree with the proposed definition for Reportable Attempted Cyber Security Incident and offers an alternative below.

APPA's concern with the proposed definition is due to the use of, "one or more reliability tasks of a functional entity." The proposed definition of Reportable Attempted Cyber Security Incident and that term, introduce ambiguity in determining attacker intent, making it difficult to determine if an attacker intended to compromise or disrupt one or more reliability tasks.

For example in the event of a ransomware attack that affected an EMS workstation – it would be difficult to distinguish if this was an attempt to compromise or disrupt a reliability task, or was the attacker's intent financial gain? The following definition attempts to eliminate this concern:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:
· the operation of a BES Cyber System; or
· Electronic Security Perimeter; or
· Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

Likes 0	
Dislikes 0	

Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	

We agree with EEI's comments for this question.

Likes 0	
Dislikes 0	

Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports EEI's comments. The term “attempts to compromise” could be construed as vague because it does not clearly define what constitutes a reportable attempt, which could create an undue reporting burden on entities without a commensurate reliability benefit. Many entities receive thousands of attempts to comprise their networks daily, and most have nothing to do with the EMS system. The standard should make clear that “attempts” of that kind should not be reportable.	
Likes 0	
Dislikes 0	

Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Currently, NERC does not define what an “Attempt” is. An “attempt” could vary from entity to entity depending on how an individual defines the term. The language “attempt” could be comprised of anything; the wording of a “Cyber Security Incidents that compromise, or “attempt” to compromise, a responsible entity’s ESP or associated EACM…”is vague and ambiguous. Not only does “attempt” needs to be defined so does “detected. If one perceives there to be an “attempt” what are the measures/definition for “detecting” the “attempt.”	
Likes 0	
Dislikes 0	

Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC	
Answer	No
Document Name	
Comment	
Definitions do not limit what must be reported. Entity will need to devote significant resources to reporting – which takes away resources from addressing cyber attacks	

Some concern with “Reportable Cyber Security Incident” for field locations (substations & generators) since these locations have fewer defense layers.

Concerns that the “Cyber Security Incident” puts the burden of determining intent – is the intent to “compromise” or “disrupt.” Expect this lack of clarity to result in in over-reporting which makes finding the real incident akin to a needle in the haystack.

Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam
Dislikes 0	

Response

David Maier - Intermountain REA - 3

Answer	No
Document Name	

Comment

The issue with this draft is the potential for application inconsistency based on what is assumed to be an “attempt”. Neither “Attempts to compromise” nor “attempt” have been defined by the SDT.

1. attempt” should be properly defined by the SDT to remove ambiguity. In defining what constitutes an attempt, the SDT may require evidence of intent and relate all actions and packets from a campaign as a single attempt report.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

The concerns about expanding the scope of EACMS into CIP-003-6 (or -7) appear to be misplaced. The requirements that are applicable to EACMS are clearly identified in the “Applicable Systems” column in each Requirement table. Even if Low Impact Cyber Assets should meet the definition of EACMS, they would not be subject to those related requirements unless explicitly included in the corresponding “Applicable Systems” column. Mixing applicability of EACMS into a Term definition goes against norms established in the rest of CIP Standards, regardless of whether “High or Medium Impact” is also added. Suggest removing “High or Medium Impact” from the CSI definition.

The concept of Reportable Attempted Cyber Security Incident (RACSI) and the resulting definition of “Reportable Cyber Security Incident” (RCSI) is unnecessarily complicated, counter-intuitive, and results in unnecessarily verbose additions to the requirements. The term “Cyber Security Incident” (CSI) includes both attempted and “successful” cases of being disrupted/compromised. RCSI is confusing because it adds to CSI reporting requirements but subtracts the attempted incidents, with only the former reflected in the name. As such, the name “RCSI” erroneously suggests it

includes all CSI that meet additional reporting requirements. A more complete name might address this concern however this doesn't address the remaining concerns.

The proposed RSCI and RACSI terms separate out attempted and "successful" reportable CSI, which results in having to name both whenever referencing reportable CSI. This results in the need to repetitively insert "Reportable Attempted Cyber Security Incident" after "Reportable Cyber Security Incident" 14 times (including the missed additions in M4 and probably R4.1). The only standalone use of RACSI occurs in R4.3 to specify the different reporting timelines. A more concise and intuitive approach would be to define RCSI only as the CSI that meet the conditions that make it reportable (ie. Not PSP related) and thus include both attempted and "successful" CSI.

This would avoid the need to verbosely replace "RCSI" with "RCSI and/or RACSI" the 14 times. It is suggested that RACSI be abandoned and instead a new term should be adopted that encompasses the RCSI that meet the additional Compromising or Disruptive criteria. Possible names might include variations including "Compromise" or "Disrupt" (C/DRSCI? RC/DSCI?) but seem unwieldy. Incorporating the word "successful" as used above is unhelpful because it is a so called "success" only from the attacker's perspective. We suggest using the term "Reportable Cyber Security Attack" (RCSA), which describes both variations while clearly and concisely indicating it is more serious than a mere RCSI. Other names might be more appropriate, but we will use RSCA for the rest of this comment.

The advantages of using the existing CSI, the redefined RSCI, and the new RSCA terms would be:

· they build on each other intuitively

· a single term exists to express the context mentioned by each (sub-)requirement. (ie. No need to list combinations of CSI, RCSI, or RCSA in the text of any (sub-)requirement)

In addition to the above concerns, the proposed CSI, RCSI, and RACSI definitions use similar but differently worded inclusions that is unnecessarily complicated and may lead to unintended interpretations. For CSI, consider:

· Reference to ESP and EACMS seems redundant as what component of an ESP is not an EACMS? And all EACMS are being included in the "Applicable System" column anyway. EACMS do not need to be mentioned in the definitions.

For RCSI and RACSI, consider:

· By definition, a BES Cyber System (BCS) embodies one or more "reliability tasks" and under CIP-002, all such cyber assets supporting those tasks must be grouped into a BCS. Therefore the "Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System" in CSI is equivalent to "One or more reliability tasks of a functional entity" in RSCI/RACSI. Why should RSCI/RCSA be based on CSI but then restate this?

· Use of the words "compromise" and "disrupt" are inconsistent. CSI applies only "compromise" to the first inclusion and "disrupt" to the second. RSCI/RASCI uses "compromised or disrupted" for all of its inclusions, however it is limited to only the inclusions that exist for CSI, so the RSCI/RASCI inclusions appear broader than they are. For instance, a non-disruptive compromise of a BCS cyber asset would not be included by the proposed RSCI/RASCI definitions because it doesn't meet the CSI inclusions.

· Redefinition of EACMS (functions 1-5) seems entirely redundant and should be removed even though that terminology was used by FERC in its order. Even if EACMS includes some unlisted function other than the 5 mentioned, it would still be included by the fact that all EACMS are being added to the "Applicable Systems" column.

The logical intersection of RCSI or RACSI definition with CSI definition and inclusion of above considerations leaves RCSI/RACSI with effectively only the following much more narrow inclusions:

· Disruption of a BCS

· Compromise of an ESP

The following proposed term definition approach captures the intent of the drafted definitions without the confusing parallel language:

CSI: A malicious act or suspicious event that attempts or succeeds in compromising or disrupting:

· a reliability function of a BES Cyber System

· an ESP

· a PSP

RCSI: A CSI where the compromise or disruption has been confirmed, excluding those incidents that solely involve a PSP.

RACSI: A CSI where the compromise or disruption has not been confirmed, excluding those incidents that solely involve a PSP.

BCS applicability (High, Medium, Low) and related EACMS still identified in the “Applicable Systems” as per convention.

The phrasing also ensures when a CSI involves both the cyber and physical aspects, the CSI is still reportable.

If combined with the earlier suggestion of using alternate terms CSI, RCSI, and RCSA, the definitions could be as follows or similar:

CSI: Same as above approach.

RCSI: A CSI for which the actual or attempted compromise or disruption does not solely involve the PSP.

RCSA: A RCSI for which the compromise or disruption is confirmed to have occurred [rather than merely be attempted]

Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	

With regard to the proposed definition of “Cyber Security Incident”, the notion of attempts seems to be left to the responsible entity to define as part of process development. The SWG proposed the following categories of attempts at compromise of the BES for responses to the NOPR (Docket Nos. RM18-2-000 and AD17-9-000) : “…Some criteria for events and incidents that should be reported include:

- If discovered, persistent compromise and attempts to pivot to critical systems could be interpreted as facilitating effort to harm reliable operation.
- Insider incidents involving access to ESP’s.
- Incidents involving ICS systems (such as ICCP network or server equipment).
- Incidents involving Physical access that could involve BES Cyber Systems.
- Events and incidents noted as involving ESP’s.
- Incidents with progress along a kill chain to the Modify/Install step (reference: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf). “

It may be that such lists of criteria for categories of attempts belong in Implementation Guidance more than the standard requirement language itself. The drafting team should include language in either the standard or the guidance to clarify the role of the responsible entity in defining attempts in a manner that lends itself to effective compliance monitoring.

In the definition of Reportable Cyber Security Incident, the SWG proposes that Electronic Access Control or Monitoring System (EACMS) not be limited to specific functions. This will enable clear use of existing categorization of cyber assets without confusion or added burden of sub-categorization for EACMS cases.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	No
Document Name	

Comment

Grammatical Issues: The draft definition for Cyber Security Incident contains a typographical error that should be fixed prior to final ballot. The terms should be “Electronic Access Control or Monitoring System for High or Medium Impact BES Cyber Systems.”

Additionally, the definitions of Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident should reference EACMS consistent with the general definition of Cyber Security Incident: “Electronic Access to Control or Monitoring System (EACMS) for High or Medium Impact BES Cyber Systems that provide the following functions…”

Substantive Issues: The proposed definitions of “Cyber Security Incident” and “Reportable Attempted Cyber Security Incident” includes the language “attempt to compromise or disrupt” as an element of the condition. The statement “attempt to compromise or disrupt” is unclear, ambiguous, and should be further defined by criteria. The SSRG supports the following categories proposed by the SWG in its comments:

{C}· If discovered, persistent compromise and attempts to pivot to critical systems could be interpreted as facilitating effort to harm reliable operation.

{C}· Insider incidents involving access to ESP’s.

{C}· Incidents involving ICS systems (such as ICCP network or server equipment).

{C}· Incidents involving Physical access that could involve BES Cyber Systems.

{C}· Events and incidents noted as involving ESP’s.

{C}· Incidents with progress along a kill chain to the Modify/Install step (reference: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf). “

Does this need to address entity definition of attempt (confirmed attempt?). Does the exclusion of PSP attempts and disruption make sense as far as reporting goes? PSP’s would seem to be as important as ESP’s in this regard.

With regard to the proposed definition of “Reportable Cyber Security Incident”: Should this simply be EACMS without restriction or one of other descriptions of EACMS?

With regard to the proposed definition of “Reportable Attempted Cyber Security Incident”: Is this definition needed given the prior definitions (note “attempt” shows up in Cyber Security Incident already)?

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	No
Document Name	2018_ 02_ CIP 008 6_ 102218 Final Comments.docx

Comment

Comments: The current draft does not provide clarity on what constitutes an attempt. Attempt is not a defined term and does not identify that the entity may come up with a methodology or approach on what constitutes an attempt. Including attempt “as is” leaves room for differences of opinion on what an attempt is and could be interpreted differently among entities and auditors. Exelon suggests including a requirement for entities to develop a process to define attempts. A defined term may be overly prescriptive, and inhibit the evolution of information sharing. Separately, the standard drafting team should clarify the Cyber Security Response obligations related to PSPs by removing Physical Security Perimeters from Cyber Security Incident definition unless its paired with the breach to an ESP or EACMS. As the proposed Cyber Security Incident definition reads, it could be interpreted that a PSP breach alone constitutes a Cyber Security Incident

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy recognizes and supports the good work that the CIP-008-6 Standards Drafting Team (SDT) has done in addressing the Commission's objectives, identified in Order 848, for modifications to Cyber Security Incident Reporting. While Xcel Energy generally agrees with the SDT's direction, we believe that some further clarification is needed for the proposed definitions for Cyber Security Incidents, Reportable Cyber Security Incidents, and Reportable Attempted Cyber Security Incidents. To remedy the lack of clarity we believe exists around these terms Xcel Energy suggests the following three changes be made:

1. Retirement of the term Cyber Security Incident
2. Modify the term Reportable Cyber Security Incident to read as follows:

Reportable BES Cyber Security Incident:

A malicious act or suspicious cyber event that compromises an Electronic Security Perimeter or Electronic Access Control or Monitoring System (EACMS) of a High or Medium Impact BES Cyber System or; compromises or disrupts the operation of a High or Medium Impact BES Cyber System.

3. Modify the new term Reportable Attempted Cyber Security Incident to read as follows:

Reportable Attempted BES Cyber Security Incident:

A malicious act or suspicious cyber event that was an attempt to compromise an Electronic Security Perimeter (ESP) or Electronic Access Control or Monitoring System (EACMS) of a High or Medium Impact BES Cyber System or; was an attempt to compromise or disrupt the operation of a High or Medium Impact BES Cyber system.

If the SDT opts to keep all three definitions, Xcel Energy would suggest they be changed to read:

BES Cyber Security Incident:

A malicious act or suspicious event that:

- *Compromises, or was an attempt to compromise the Electronic Security Perimeter or Electronic Access Control or Monitoring System for High or Medium Impact BES Cyber Systems; or*
- *Disrupts, or was an attempt to disrupt, the operation of a BES Cyber system*.

Reportable BES Cyber Security Incident:

A BES Cyber Security Incident that results in an actual compromise or disruption

Reportable Attempted BES Cyber Security Incident:

A BES Cyber Security Incident that was an attempt to compromise or disrupt

The suggested changes above are based on the following issues identified by Xcel Energy:

- Xcel Energy removed the list of EACMS in the above suggested definitions. It is our belief that listing the types of EACMS that apply is redundant. The only EACMS that would have been excluded would have been intermediate systems. However, by including any EACMS that have IRA we have brought intermediate systems back into scope. Also, if the type of EACMS in scope needs to be incorporated, inserting it in these definitions may be problematic. If the distinction needs to be made about the types of EACMS, we suggest it be contained with the Standard itself.
- Xcel Energy is also concerned with the inclusion of "one or more reliability tasks of a functional entity" as it is superfluous and very vague. The use of the term is already contained in scope of CIP-002. The inclusion of the term BES Cyber Systems in the proposed changes to definitions above incorporates the intent of including the "one or more reliability tasks of a functional entity" language. It would be best to remove this wording to avoid any undue confusion that could result.

- The current definition of a Cyber Security Incident includes language for the attempt or compromise of a Physical Security Perimeter (PSP) and the modified definition includes the references to PSPs as well. However, all reporting Requirements and definitions of Reportable Cyber Security Incidents and attempts exclude PSPs. This leads us to inquire what the role of a PSP in a Cyber Security Incident is. Physical Security compromises are already reported under EOP-004 R2 to law enforcement. Responsible Entities could report on compromises to Physical Access Control Systems but those were not included in the FERC Order 848. Xcel Energy would recommend removing references to Physical Security from the proposed modification to the Cyber Security Incident definition. Or the Standard Drafting Team should identify the role the PSPs have in a Cyber Security Event and when they do not need to be reported under the requirements.

- Xcel Energy believes the BES should be added to the definitions for Cyber Security Incidents, Reportable Cyber Security Incidents, and Reportable Attempted Cyber Security Incidents. Xcel Energy notes that a "cyber security incident" is a common term used broadly across many industries and throughout the Xcel Energy enterprise, with the term already existing in many policies, plans, and procedures that do not apply to a BES. NERC's use of the term applying strictly to incidents affecting the BES creates clarity issues in documentation that uses the term more broadly. Xcel Energy uses an enterprise wide cyber security center that monitors, investigates, and responds to all types of cyber security events, regardless of their BES designation. Using common terminology and only applying it to events that affect BES systems will make it more difficult to internally differentiate between those incidents that relate to the BES and those that do not. Adding BES to these terms will allow Responsible Entities to update internal documentation in such a way to avoid confusion events and appropriate responses to those events.
- In the modified term for Cyber Security the new (3) lists "Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;" The "of" should be removed and replaced with "or."

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Need to draw some boundaries around what does (and does not) constitute an attempted compromise. Too burdensome on small entities with no "floor" on what might constitute an attempted compromise.

Likes 0	

Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	

Comment
Vectren agrees with the modified definitions of Cyber Security Incident and Reportable Cyber Security Incident. However, the new definition of Reportable Attempted Cyber Security Incident is very broad which leaves it open to interpretation. This definition as written will cause an unreasonable administrative burden on the entity, requiring us to dedicate significant time and resources to track and investigate potential attempts. By investigating blocked attempts, the focus is shifted away from higher risks. The resources of E-ISAC and ICS-CERT will also be impacted by a larger volume of reports regarding lower risk threats including the potential attempts to compromise. Ultimately, this shift in focus could lead to a compromise of safety and reliability of the BES. Recognizing the task of the SDT to draft a reasonable definition, the definition in its present form will not serve the intent of the FERC Order No. 848 directive. We would suggest the SDT narrow the scope of “attempts to compromise” within the definition to alleviate the potential burden to the entity, E-ISAC and ICS-CERT.

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
Without additional parameters around the specifics of what constitutes an “Attempt to Compromise”, Southern Company asserts that the requirements are painted with too broad a brush. Further defining “Cyber Security Incident”, “Attempt to Compromise”, “Reportable Attempted Cyber Security Incident”, and “Reportable Cyber Security Incident” will allow Registered Entities the opportunity to meet the standard in a clear and measurable way. See below for alternate definitions that clarify the meanings and alleviates ambiguity contained within the current proposed definitions. Notably, Southern Company does not agree with the proposed definition of “Reportable Attempted CSI” (RACSI). The new defined term still fails to establish the parameters for what is “reportable” and should focus solely on the threshold that turns a CSI into a Reportable Attempt. If the definition of CSI is substituted where used within RACSI, it is very unclear. We suggest that this definition not have a subject of “Cyber Security Incident” since it appears that the RACSI definition is a repeat of CSI minus PSPs. We suggest that instead of repeating most of the definition of CSI and also using the CSI term as the subject, this definition should instead focus solely on the *threshold* that turns a CSI, which already includes attempts, into a Reportable Attempt. Southern Company proposes the following alternate definitions for use in CIP-008:

Cyber Security Incident – "***an unconfirmed*** malicious act or suspicious event ***requiring additional investigation to determine if it:***

- Compromis***ed***, or was an attempt to compromise the ESP or PSP, or
- Disrupt***ed***, or was an attempt to disrupt the operation of a BES Cyber System ***or associated EACMS***"

Reportable Attempted Cyber Security Incident – "a ***confirmed*** malicious act that:

- Was ***determined by the Responsible Entity to be*** an attempt to compromise the ESP, or
- Was ***determined by the Responsible Entity to be*** an attempt to disrupt the operation of *a* ***high or medium impact*** BES Cyber System ***or associated EACMS****."*

Note: Once confirmed by the Responsible Entity, the incident must be reported within the prescribed timeframes.

Reportable Cyber Security Incident - a ***confirmed*** malicious act that has compromised or disrupted one or more reliability tasks of a functional entity.

* See comments in our response to Q2 regarding the creation of a new NERC defined term "EACS".

Using the above definitions, CSI is an event that appears to potentially be malicious or suspicious and must be investigated further as per existing requirements. Once a determination is made that the event was actually targeting or attempting to compromise a BES Cyber System, or associated ESP or EACMS (for high and medium impact BCS), the event then falls into one of the two reportable categories depending on the level of success in the attempted or actual compromise, and the impact classification of the compromised asset(s). The proposed modifications shown above maintain proper scoping of reporting "attempts to compromise" at the high and medium impact BCS and associated EACMS level and does not impact the current use of the CSI and RCSI defined terms as they apply to CIP-003 R2, Attachment 1, Section 4.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Reclamation recommends the proposed definition for Reportable Attempted Cyber Security Incident be expanded to include disruption or attempted compromise of Physical Security Perimeters and Physical Access Control Systems. This would allow identifying a Facility as a potential target without its reliability or operations being affected.

Reclamation also recommends removing the following language from the bullet point for EACMS because it is redundant of the EACMS definition: *"that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting."*

Therefore, Reclamation recommends the proposed new term be changed

from:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:

- One or more reliability tasks of a functional entity; or
- Electronic Security Perimeter; or
- Electronic Access Control or Monitoring System (EACMS) that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting

to:

Reportable Attempted Cyber Security Incident:

A Cyber Security Incident that was an attempt to compromise or disrupt:

- One or more reliability tasks of a functional entity; or
- Electronic Security Perimeter (ESP); or
- Physical Security Perimeter, including locally-mounted hardware or devices; or
- Physical Access Control Systems (PACS); or
- Electronic Access Control or Monitoring System (EACMS).

If the above solution is not accepted, Reclamation asserts the following:

The proposed definition of a Cyber Security Incident includes compromise or attempted compromise of a Physical Security Perimeter (PSP), but in Part 4.1 the report excludes PSPs. For example, if a PSP was breached and no BES Cyber Systems were compromised, then there was not actually a Cyber Security Incident. The breach may have been due to theft or vandalism not involving BES Cyber Systems.

The Reportable Attempted Cyber Security Incident definition needs to be consistent with the current version of the standard, CIP-008-5 R1.1, which requires each entity to have a process to identify if a malicious act or suspicious event was an attempt to compromise the Electronic Security Perimeter. If the intent is to only report incidents that actually compromise cyber equipment, Reclamation recommends the Cyber Security Incident definition be changed to:

A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise (1) the Electronic Security Perimeter or (2) Electronic Access Control of Monitoring System for High or Medium Impact BES Cyber Systems, or;

- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

Reclamation also recommends removing “Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter,” from Requirement R4 Part 4.1 so it reads:

Initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted.

Likes 0	
Dislikes 0	

Response

2. The SDT added Electronic Access Control or Monitoring System (EACMS) to applicable systems as opposed to modifying the NERC Glossary EACMS definition to ensure the FERC Order No. 848 paragraph 54 directive to expand reporting requirements to EACMS was met without expanding the scope into CIP-003 (low impact BES Cyber Systems) or CIP standards that use the existing EACMS NERC Glossary definition. Do you agree with the addition of EACMS to the applicable systems column in the tables in CIP-008-6? If not, please provide comments and an alternate approach to addressing the directive, if possible.

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
While Xcel Energy agrees with adding EACMS to the Applicable Systems column in the Requirement tables, we would like to express our concern with the effect of adding certain monitoring and alerting systems as applicable EACMS. If we are required to monitor our monitoring systems for Cyber Security Incidents and Attempted Cyber Security Incidents, then shouldn't we also need to monitor that monitoring system? It is not clear to Xcel Energy where the line of succession for reporting on monitoring and alerting systems would conclude. The addition of monitoring systems creates a "hall of mirrors" effect. Xcel Energy asks the Standard Drafting Team to address the hall of mirror issue with appropriate language in the Requirement.	
Likes 0	
Dislikes 0	
Response	

Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
NC	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC	
Answer	Yes
Document Name	
Comment	

We agree that adding EACMS is a step in the right direction.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	Yes
Document Name	

Comment

We agree that adding EACMS is a step in the right direction

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	Yes
Document Name	

Comment

Texas RE agrees with the addition of EACMS to the applicable systems column in the tables in CIP-008-6. Please see Texas RE's comments to question #1 regarding the definition.

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1, Group Name Exelon Utilities	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Douglas Johnson - American Transmission Company, LLC - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5;	

Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	

Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	

Comment
Reclamation recommends the SDT use existing terms from the NERC Glossary or follow procedures for adding new terms to the NERC Glossary of Terms. Instead of stating the EACMS example in the requirement, the EACMS definition should be revised as follows: Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems. *Examples include Cyber Assets that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting."*

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 Company feels the unnecessary inclusion of cyber assets that are used solely to perform a "monitoring and alerting" function is an undue burden to entities as they have been confirmed to have little to no impact on BES reliability. In NERC's comments to FERC in response to the associated FERC NOPR, NERC stated[1]: *"Additionally, as the term EACMS covers a wide array of devices that perform different control or monitoring functions, the various types of EACMS present different risks to BES security. As such, it may be necessary to differentiate between the types of EACMS to ensure that any reporting requirement is scoped properly. NERC thus respectfully requests that the Commission provide NERC the flexibility to define "attempts to compromise" and differentiate among EACMS, as necessary, to ensure that any reporting obligation is designed to gather meaningful data without overburdening entities."* *"given the wide array of EACMS, it may be beneficial to limit the types of EACMS subject to any reporting requirement to scope the requirement appropriately."* *"while NERC is supportive of the general scope proposed by the Commission, NERC recognizes that there is still a need to refine the scope of the proposed directive to ensure that it would provide meaningful data without overburdening entities. NERC identified at least two items that require additional focus."* *"Second, as defined in the NERC Glossary, EACMS include a wide variety of devices that perform control or monitoring functions. The risks posed by these various systems may differ substantially. It is important to focus industry resources on higher risk systems. Certain devices that qualify as EACMS*

may have no or minimal impact on the security of BES Cyber Systems if compromised. NERC thus needs to consider whether to define the reporting threshold to differentiate between the various types of EACMS for reporting purposes."

"For these reasons, NERC respectfully requests that the Commission provide NERC the flexibility to refine the thresholds for reporting, including defining "attempts to compromise" and differentiating between EACMS, as necessary, to ensure that any reporting obligation is designed to gather meaningful data without overburdening entities."

Despite FERC's position and language used in the Final Order, Southern feels additional discussion is needed between NERC and FERC to avoid unnecessarily scoping in systems that, if compromised, do not have a direct impact on the BES. Failing to realize this fact could hinder existing NERC SDT efforts in the realm of development of new requirements to address virtualization and other technological advancements.

Southern Company supports the Project 2016-02 SDT that is also working on redefining the EACMS definition to address virtualization and other technological advancements, and we strongly encourage the Project 2018-02 SDT to work together with them on this. Working on establishing this alignment between SDTs now will help alleviate the need in the future to modify standards again.

[1] NERC Filings to FERC DL_NERC_Comments_Cyber_Security_Incident_Reporting, Page 2, Paragraph 1.

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

While Vectren agrees that adding EACMS to the scope is a good security practice, it is not clear how entities would meet the requirement without a more focused definition of Reportable Attempted Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

David Maier - Intermountain REA - 3

Answer	No
Document Name	

Comment

Applying this as reportable only to EACMSs implies that an *attempt to compromise* an EACMS is reportable but an *attempt to compromise* a BCA is not. "Attempt to compromise" must be defined and mitigating controls and monitoring should be applied to all assets and in uniform fashion.

Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Add the list of functions noted in the FERC order, to define the in-scope terms. The FERC Order as follows: “and their associated EACMS that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.” We appreciate that this FERC clarification is in the definitions of Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident. However, requirement part 1.1, for example, is only about Cyber Security Incidents for which the definition does not contain this FERC clarification. Therefore, as proposed, the scope of EACMS is different for this requirement part. For consistent scoping, the five functions should be added to the EACMS reference in all of the CIP-008 requirements’ applicable systems.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No
Document Name	

Comment
While Vectren agrees that adding EACMS to the scope is a good security practice, it is not clear how entities would meet the requirement without a more focused definition of Reportable Attempted Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

Scott McGough - Georgia System Operations Corporation - 3	
Answer	No
Document Name	

Comment
GSOC is concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, GSOC believes that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team's approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. GSOC urges the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	No
Document Name	

Comment
Agree with NPCC comments

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We are concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, we believe that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team's approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. We urge the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA is concerned with the broad expansion of the two draft modified definitions and the same with the draft new definition. In these draft definitions and many other places in CIP-008-6 the inclusion of EACMSs is directed by FERC in Order No. 848; however, NRECA believes that FERC provided NERC and the drafting team the opportunity to further analyze the five functions FERC identified to determine and provide support for inclusion of an appropriate subset of EACMSs to be applicable to the modified and new requirements. In this first draft of the definitions and other modified and new requirements, the drafting team's approach is to include essentially all EACMSs without providing criteria for determining the appropriate applicable subset of EACMSs addressed in the modified and new requirements. NRECA urges the drafting team to undertake analysis to determine what EACMSs should be applicable in order to protect the reliability of the BES. This is especially important for the Reportable Attempted Cyber Security Incident definition and related reporting requirements as it will require a report for every packet denied by a firewall, making this requirement overly burdensome for entities without a commensurate benefit to the reliability of the BES and BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	No

Document Name	
Comment	
The proposed changes and new definitions should be confirmed prior to expanding the reporting requirements to additional assets.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
This reference to EACMS also should include the five functions described in the FERC Order as follows: “and their associated EACMS that provide any of the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting.” We appreciate that this FERC clarification is in the definitions of Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident. However, requirement part 1.1, for example, is only about Cyber Security Incidents for which the definition does not contain this FERC clarification. Therefore, as proposed, the scope of EACMS is different for this requirement part. For consistent scoping, the five functions should be added to the EACMS reference in all of the CIP-008 requirements’ applicable systems.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP recommends an adjustment from ECAMs to EAC systems because monitoring systems are not as critical and having the ECAMs monitored by a separate system will incur additional costs and resources.	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	

Answer	No
Document Name	
Comment	
Definitions should not include EACMs. Every packet denied by a firewall would generate a potential Reportable Attempted Cyber Security Incident, making this requirement onerous for the entities.	
Likes 0	
Dislikes 0	
Response	

3. Do you agree with reporting timeframes included Requirement R4? If you disagree please explain and provide alternative language and rationale for how it meets the directives in FERC Order No. 848.

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

Answer	Yes
Document Name	

Comment

TVA agrees with the proposed reporting timeframes only if the definition of “attempted” is appropriately clarified based on TVA’s comments to Question 1.

Likes 0	
Dislikes 0	

Response

larry brusseau - Corn Belt Power Cooperative - 1

Answer	Yes
Document Name	

Comment

Assuming there is no measurable impact on risk, I recommend updating R4.2 and R4.4 from 5 days to 7 days, so that updates could be made on a weekly basis. I recognize these reports are not intended to be a regular occurrence, but also recognize that the reporting frequency could support this consideration.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

None

Likes 0	
Dislikes 0	

Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Assuming there is no measurable impact on risk, we recommend updating R4.2 and R4.4 from 5 days to 7 days, so that updates could be made on a weekly basis. We recognize these reports are not intended to be a regular occurrence, but also recognize that the reporting frequency could support this consideration.	
Likes 0	
Dislikes 0	

Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Please see comment on #4, below, regarding risk for meeting the 1 hour reporting deadline. For Reportable Attempted Cyber Security Incidents, we suggest the deadline is changed from the next calendar day to the next business day.	
Likes 0	
Dislikes 0	

Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
See comments from the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	

Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
ATC agrees the reporting timeframes are reasonable; however, because Reportable Attempted Security Incidents constitute a condition where security controls operated as designed and prevented an actual compromise or disruption, ATC supports further SDT consideration of a longer timeframe for preliminary reporting of Reportable Attempted Security Incidents to balance the risk, timely reporting, and administrative burden. Additionally, where the term 'calendar day' is used, ATC requests the SDT consider adding the qualifier, of '11:59 pm local time' for ultimate clarity on the reporting deadline.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
The companies recommend replacing "5 calendar days" with "5 nonholiday weekdays." The recommendation is to avoid required follow-up reporting to fall on a weekend or holiday.	

Also, we do not believe occasionally extending a follow-up reporting period to seven or eight days is detrimental to the reliability of the BES.	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Santee Cooper agrees that the time for reporting a Reportable Attempted Cyber Security Incident should be different from that of a Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
This is reasonable and adds flexibility because the requirement makes it clear that 1) the timeframe is based on when the incident is determined to be reportable and 2) attribute information does not need to be submitted until it can be determined. Also, the requirement lets entities update attribute information when revised information becomes available.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	

NC	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
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	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	

Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Xcel Energy believes that reporting updates stemming from a Reportable Cyber Security Incident would be better reported on a weekly (7 calendar days) basis after the initial notification. Entities will learn additional details of a Cyber Security Incident as the investigation evolves over time. Reporting each new item learned each time it is learned would create an administrative burden. Gathering information and reporting over 7 calendar days would allow for a more uniform internal process and regular timely reporting.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
See comments of the ISO/RTO Council.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment
There is ambiguity in when the reporting timeframes begin. Additional language should be added that clarify that the timeframes do not begin until the entity has concluded it's investigation and made a determination on the attempt or actual penetration. The current language could be interpreted differently and could lead to inconsistent results in determining when an attemptm or actual penetration should be reported.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
Seminole does not agree with the inclusion of EACMs in R4. See comments above.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
SRP agrees with the 1 hour and 1 day for initial reporting. Reporting if attributes change within 5 days will add administration burden of having the template attachment completed. SRP recommends an adjustment to when the investigation is complete so a complete investigation with all the facts are presented in the template attachment. There is a concern with more reports of Reportable Attempted Cyber Security Incidents may dilute or mask actual real reports.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No

Document Name	
Comment	
No mention of OE-417 reporting timeframes.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
No mention of OE-417 reporting timeframes.	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	No
Document Name	
Comment	
No mention of OE-417 reporting timeframes.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	

Besides meeting CIP-008 reporting requirement, for the same event, an entity may also have EOP-004 and the Department of Energy (DOE) OE-417 reporting requirements to fulfill. These standards/regulation have different reporting requirements and reporting timeline. Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format. We recommend that an entity use CIP-008-6 proposed reporting timeline.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

Requirement parts 4.2 and 4.4 reference 5 calendar days. We recommend replacing 5 calendar days with 7 calendar days so this can be a regularly scheduled check for updated attribute information on the same day of the week, particularly if multiple updates are required.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1

Answer	No
Document Name	

Comment

Besides meeting CIP-008 reporting requirement, for the same event, an entity may also have EOP-004 and the Department of Energy (DOE) OE-417 reporting requirements to fulfill. These standards/regulation have different reporting requirements and reporting timeline. Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format. We recommend that an entity use CIP-008-6 proposed reporting timeline.

Likes 0	
Dislikes 0	

Response

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

Answer	No

Document Name	
Comment	
Updates within a prescriptive five calendar day or other period when attributes change or are known to E-ISAC present an unreasonable expectation on an entity. Initial reporting and final reporting upon conclusion of analysis of determination of all attributes on the entity's timeline should be the preferred basis.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	
Based on our comments for question 1 to revise the existing Reportable Cyber Security Incident rather than creating an additional one, the timeline can be the same as before.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
The language, "And Reportable Attempted Cyber Security Incidents" should be removed from R4.	
Likes 0	
Dislikes 0	
Response	
Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	No

Document Name	

Comment

It is recommended that all reporting timelines fall in line with established Reporting Procedures established by current federal reporting guidelines see US-CERT Federal Incident Notification Guidelines.. ALSO: Reclamation agrees with the proposed reporting timeframes.

Reclamation recommends the following language be deleted from R4 Part 4.1 when the definition of Reportable Attempted Cyber Security Incident is modified to include PSPs: *"Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter …"*

Therefore, Reclamation recommends R4 Part 4.1 be changed

from:

Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter, initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted.

to:

Initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3

Answer	No
Document Name	

Comment

The one-hour timeframe for Reportable Cyber Security Incidents seems ressonable because they are critical events. However the "end of next calendar day" requirement for Reportable Attempted Cyber Security Indicents seems unnecessarily stringent. Because attempted incidents are not critical events, changing the timeframe for them to "end of next business day" would allow Entites to meet the intention of the reporting requirement without the need for additional resources to review, analyze, and report on non-cricital events that occur on weekends and holidays.

Likes 0	

Dislikes 0	

Response

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	No
Document Name	

Comment
We strongly encourage NERC and the SDT to reconsider requiring each Responsible Entity (RE) to report to two different agencies (E-ISAC and ICS-CERT). If NERC cannot coordinate with both agencies to have one central reporting mechanism, we would recommend expanding the timeframe to allow for one hour per agency, which would change the R4.3 requirement to: *"Timeline for initial notification: **Two hours** from the determination of a Reportable Cyber Security Incident. **48 hours** after determination of a Reportable Attempted Cyber Security Incident."* Rationale behind this suggestion can be illustrated with the following example: If an RE decides to contact the E-ISAC as the first agency and makes a phone call for initial notification, but is placed on hold for an extended time, it is possible that reporting to the ICS-CERT (as the second agency) may fall outside of the one hour window. We believe that by doubling the reporting agencies REs should receive double the amount of time to report.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	

Comment
The timeframe for Reportable Attempted Cyber Security Incidents could extend to almost a 48 hr period. As a reportable attempted incident, 48 hours is quite a long time and shortening this window could help EISAC increase responsiveness across regions or entities that could also be impacted. RF recommends the SDT consider revising the timeframe to be the same as or within 24 hrs from determination of Reportable Cyber Security Incidents. For example, if either event reaches the threshold of "reportable", it is recommended to have the same notification window—for consistency, ease of understanding and also to enable the industry to be proactive and prevent a potential incident from becoming an actual compromise. Why have 2 different timeframes based on the definitions between "confirmed" and "attempted"? Also, from a entity perspective, it would be easier for them to have "one" reportable notification process and timetable rather than splitting hairs based on definitions. And, most entities would likely utilize a singular notification process and report it under the same time and conditions because they wouldn't want to wait or have to create and follow separate processes.

Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA does not have comments on the timeframe at this time due to needing our concerns with Questions 1 and 2 being addressed first. Once the EACMS concern we identified are addressed we will then provide feedback on the timeframes.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Utility Services agree with APPA's comments. In addition, we are concerned with the formatting of the timeline list. Tyically, bullets indicate an "or" statement, but the way the items are phrased indicates "and". If "or" is the intended phrasing, we propose the following change: Timeline for initial notification: • One hour from the determination of a Reportable Cyber Security Incident; or • By the end of the next calendar day after a determination of a Reportable Attempted Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	

We do not have comments on the timeframe at this time due to needing our concerns with Questions 1 and 2 being addressed first. Once the EACMS concern we identified are addressed we will then provide feedback on the timeframes.

Likes 0	
Dislikes 0	

Response

Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6

Answer	No
Document Name	

Comment

Section 4.3 – Next calendar day seems very aggressive. Would it be better to align this with the 15 day requirement currently used in other NERC CIP documents

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

More time may be needed to support a more complete investigation. Complex incidents will probably require more than five calendar days

We request clarification on “attempt” in Reportable Attempted Cyber Security Incident. Our answer to this question depends on the interpretation of “attempt” in the new term Reportable Attempted Cyber Security Incident. Attempt can be broadly interpreted so that an Entity could be constantly submitting this notification.

Likes 0	
Dislikes 0	

Response

Scott McGough - Georgia System Operations Corporation - 3

Answer	No
Document Name	

Comment
GSOC does not have comments on the timeframe at this time due to needing our concerns with Questions 1 and 2 being addressed first. Once the EACMS concern we identified are addressed we will then provide feedback on the timeframes.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	

Comment
A reporting timeframe of one hour is unreasonably short due to the details requested and various organizations required to receive the reports.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	

Comment
Duke Energy suggests that 7 calendar days to submit any new or changes in attribute information is more reasonable. Having a full week to further investigate and submit any new or changed attribute information could reduce the number of subsequest reports, as well as reduce hardships if an attempted incident is discovered on or near a weekend. Also, the language used in R4 could likely create confusion or unnecessary work in order to identify when to make subsequent reporting or when to stop reporting on any one incident. We suggest that there be some language in the requirement that gives a responsible entity the ability to determine when there is sufficient information to file an update on an initial report. Example language could include: *“Once entity determines that there is sufficient information to make subsequent reporting, it should be reported within 7 calendar days.”*

Likes 0	
Dislikes 0	

Response

Steven Sconce - EDF Renewable Energy - 5

Answer	No
Document Name	
Comment	

Does the requirement for Reportable Attempted Cyber Security Incident imply a need to maintain staff in the event an attempted attack occurs off business hours? Perhaps this could be changed to “within 1 business day” rather than 24 hours.

Likes 0	
Dislikes 0	
Response	

Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	
Comment	

FMPA agrees with the following comments submitted by APPA:

Regarding timing, APPA is concerned that the “end of the next calendar day after a determination of Reportable Attempted Cyber Security Incident,” will not provide sufficient time in some instances. Many smaller public power utilities do not have extensive Subject Matter Experts available that can analyze all attempts under such a time frame. Entities would make staff available for Reportable Cyber Security Events given that the BES Cyber System would have been compromised or misused which would warrant the appropriate investigation but such redeployment may not always be possible by the end of the next calendar day time frame.

We are also concerned by the stated timeframe in Part 4.4 of the requirement for updates if a Reportable Cyber Security Incident occurs. Appropriately done investigations take time and there may not be new updated information that can be provided within the 5 day time frame.

Likes 0	
Dislikes 0	
Response	

Jodirah Green - ACES Power Marketing - 6

Answer	No
Document Name	
Comment	

See comments in question 1.

Likes 0	
Dislikes 0	

Response

Kelsi Rigby - APS - Arizona Public Service Co. - 5

Answer	No
Document Name	Revisions to R4.4.docx

Comment

AZPS is concerned that a timed obligation to update information could lead to the reporting of unverified information that could continue to change and evolve as an investigation progresses. Such could result in regulators and the industry expending efforts that would later have little to no security or reliability value or benefits. In addition to the limited and potentially detrimental value in which such updates could result, the timing requirements of R4 divert resources from more important tasks such as containment, remediation, and forensic investigation. This seems unduly burdensome and AZPS recommends that the continuous update requirement be re-considered. Nonetheless, AZPS supports the maintenance of a reporting obligation until all attributes have been completed and submitted.

To address the need for ongoing reporting until all attributes are complete, AZPS recommends that any attributes not originally reported in Attachment 1 pursuant to requirement R4.3 be reported within 5 calendar days of the conclusion of the Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident. AZPS believes this timing is appropriate as it ensures that information that is reported and/or shared is actionable and accurate and that resources remain focused on the Cyber Security Incident until its containment and remediation is completed.

Additionally, AZPS notes that attributes initially reported could change as the investigation progresses and therefore recommends that, if there is change to an attribute that was previously reported, such updates should be reflected in the final report for notification. If the result of the Cyber Security Incident investigation indicates that an attribute is unknown, such should be reported in the final report.

AZPS recommends the language change to R4.4 shown in the attached.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No
Document Name	

Comment

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	

Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Stated in R4.2 & R4.4., suggested to update every seven (7) calendar days, not every five (5). This can be a regularly scheduled check for updated attribute information on the same day of the week, particularly if multiple updates are required.	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant	
Answer	No
Document Name	
Comment	
Luminant has concerns about the ability to meet the one-hour horizon for all three agencies that require reporting within an hour (E-ISAC, ICS-CERT and DOE). Additionally, this activity distracts from actual response activities. We do understand the value of quick reporting, especially if there is a coordinated attack that involves multiple entities. Reducing the reporting requirement back to a single report that is automatically disseminated to all relevant agencies would resolve this concern.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	

Timeline for initial notification of attempted is unreasonable at next calendar day (ie Friday or Saturday evening event). Additional days should be allowed to support a more complete investigation.

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	

Comment

Regarding timing, APPA is concerned that the “end of the next calendar day after a determination of Reportable Attempted Cyber Security Incident,” will not provide sufficient time in all instances. Many smaller public power utilities do not have extensive Subject Matter Experts available that can analyze all attempts under such a time frame. Entities would make staff available for Reportable Cyber Security Events given that the BES Cyber System would have been compromised or misused which would warrant the appropriate investigation but such redeployment may not always be possible by the end of the next calendar day timeframe.

We are also concerned by the stated timeframe in Part 4.4 of the requirement for updates if a Reportable Cyber Security Incident occurs. Appropriately done investigations take time and there may not be new updated information that can be provided within the 5 day time frame.

Likes 0	
Dislikes 0	

Response

Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5

Answer	No
Document Name	

Comment

Tacoma Power agrees with APPA comments:

"Regarding timing, APPA is concerned that the “end of the next calendar day after a determination of Reportable Attempted Cyber Security Incident,” will not provide sufficient time in some instances. Many smaller public power utilities do not have extensive Subject Matter Experts available that can analyze all attempts under such a time frame. Entities would make staff available for Reportable Cyber Security Events given that the BES Cyber System would have been compromised or misused which would warrant the appropriate investigation but such redeployment may not always be possible by the end of the next calendar day time frame.

We are also concerned by the stated timeframe in Part 4.4 of the requirement for updates if a Reportable Cyber Security Incident occurs. Appropriately done investigations take time and there may not be new updated information that can be provided within the 5 day time frame."

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

Regarding timing, APPA is concerned with the “end of the next calendar day after a determination of Reportable Attempted Cyber Security Incident.” Many smaller public power utilities do not have extensive Subject Matter Experts available that can analyze all attempts under such a time frame. Entities would make staff available for Reportable Cyber Security Events given that the BES Cyber System would have been compromised or misused which would warrant the appropriate investigation but such redeployment may not always fit in the end of the next calendar day time frame.

We are also concerned over the stated timeframe in Part 4.4 of the requirement for updates if a Reportable Cyber Security Incident occurs. Appropriately done investigations take time and there may not be new updated information that can be provided within the 5 day time frame.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	No
Document Name	

Comment

We believe that it is too difficult for the entity to report an Attempted Cyber Security Incident in the next calendar day without a more refined definition of Attempted Cyber Security Incident. Furthermore, investigations into attempted cyber security incidents can span days or weeks. Notification in the early stages of the investigation does not provide the level of detail that would make the notification valuable to the E-ISAC and ICS-CERT or registered entities.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

FERC Order No. 848 Paragraph 89 contemplates three timeframes for reporting:, which are summarized below:

- **1 hour - Detected Malware within ESP or incident that disrupted reliability tasks**
- **24 hours – Detected attempts at unauthorized access to an ESP or EACMS**
- **Monthly –Other suspicious activity associated with an ESP or EACMS**

The proposed language captures the 1 hour and 24 hour timelines, but omits the suggested monthly timeline. SCE&G recommends revising R4.3 as follows:

“Timeline for initial notification:

- **One hour from the determination of a Reportable Cyber Security Incident.**

- **By the end of the next calendar day after a determination of a Reportable Attempted Cyber Security Incident *that consisted of multiple targeted attempts to access an ESP or EACMS or to disrupt a reliability task.***

- ***All other Reportable Attempted Cyber Security Incidents shall be aggregated and reported once each calendar month*.” (The SDT should develop another attachment for this reporting.)**

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC

Answer	No
Document Name	

Comment

More time may be needed to support a more complete investigation. Complex incidents will probably require more than five calendar days

We request clarification on “attempt” in Reportable Attempted Cyber Security Incident. Our answer to this question depends on the interpretation of “attempt” in the new term Reportable Attempted Cyber Security Incident. Attempt can be broadly interpreted so that an Entity could be constantly submitting this notification.

Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam

Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

Attempted CSI should have a reporting deadline not sooner than the end of the next business calendar day.

The proposed language of R4.1 excludes any CSI that includes a physical component, even if it also has a cyber component. This is likely not intended.

Also, the Reportable Cyber Security Incident term by definition does not include PSP attracts. Why does the language of R4.1 suggest it does?

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

The timeline for a Reportable Attempted Cyber Security Incident should not be the next calendar day. More time is often required for registered entities to provide useful information to share for an attempt, and such sharing will still be timely even if not the next day. If the objective is to improve registered entity situational awareness it would be prudent to allow for multiple days to support more complete investigation. Based on an interest in complete information in the report and concern regarding needed resources to investigate attempted compromises there should be a longer timeline in such cases.

The timelines for reporting to both the E-ISAC and ICS-CERT are overly complicated. The requirement of additional reporting for attempts and updates do not provide significant value for the E-ISAC, the ICS-CERT or registered entities.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	No
Document Name	
Comment	
Exelon suggests increasing to a 4-hour reporting timeframe for Reportable Cyber Security Incidents to permit greater focus on incident response and allow additional time to facilitate reporting.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
The one hour timeframe for initial notification is consistent with CIP-008-5. “End of the next business day” for Reportable Attempted Cyber Security Incident seems reasonable and would allow for E-ISAC and and ICS-CERT to have reasonale awareness. As for the updates with 5 calendar days, this seems like a reasonable timeframe, but recommend the SDT revisit the language in Part 4.1 and 4.4. The wording between the two Parts could use further clarity.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
It is unrealistic to think that small entities have adequate staff on hand to continuously update multiple organizations about attempted cyber attack. Furthermore, a lack of coordination between E-ISAC and ICS-CERT (DHS) is not the industry's fault. Reporting to one entity should be sufficient for responsible entities.	
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 Company is concerned that the emphasis in these requirements is shifting from maintaining a reliable BES toward a focus on collecting and reporting data. This detracts from registered entities' obligation to maintain their focus on the reliable operation of the BES.

In reviewing R4, Southern Company the following clarification in the proposed Standard to more clearly address "who makes the determination." That said, we recommend in R4.3:

Timeline for initial notification:

- One hour from the **Responsible Entity's** determination of a Reportable Cyber Security Incident.
- By the end of the next calendar day after a **Responsible Entity's** determination of a Reportable Attempted Cyber Security Incident.

And in 4.4:

Responsible Entities shall submit Attachment 1 updates for the attributes required in Part 4.1 within **7** calendar days of **the Responsible Entity's** determination of new or changed attribute information. Submissions must occur each time new attribute information is available until all attributes have been reported.

As shown above, Southern Company also recommends the "update timeframe" in R4.4 to be expanded to 7 calendar days to facilitate regular and timely reporting for issues of an extended duration. Doing so will facilitate the ability for a registered entity who experiences a need to update attribute information to do so on a regular weekly schedule until all attributes have been reported.

Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends that all reporting timeframes align with reporting procedures established by federal reporting requirements, such as DHS/US-CERT Federal Incident Notification Guidelines.

When the definition of Reportable Attempted Cyber Security Incident is modified to include PSPs (as stated in the response to Question 1), Reclamation also recommends R4 Part 4.1 be changed

from:

Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter, initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted.

to:

Initial notifications and updates shall include the following attributes, at a minimum, to the extent known:

1. The functional impact;

2. The attack vector used; and

3. The level of intrusion that was achieved or attempted.

Likes 0	
Dislikes 0	

Response

4. The SDT created Attachment 1 to be used for consistent reporting and intentionally aligned the content with FERC Order No. 848 paragraphs 69 and 73. Do you agree with the content and use of Attachment 1?

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	

Comment

Recommend a reference to the NERC Glossary for identifying the Incident Type.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Xcel Energy believes that it is unclear if the Responsible Entity also needs to be identified or just the name of the person submitting the notification in Attachments 1 & 2

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	Yes
Document Name	

Comment

Exelon agrees with the form, but offers suggestions for improvement. Some considerations for scenarios when considering revisions to the form:

- Suggest addition of a field or explanation for indicating a report is the final.
- Should the form include where the incident is occurring?

- Should the time of the occurence be included on the form so other RE's could potentially assess for potential threats, on their system, around the same time as well?
- Adding information to include how/where to submit the information (ie. Email, phone number).

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	Yes
Document Name	

Comment

Reporting to multiple agencies using different forms/formats should be avoided to reduce redundancy and burden on the entities.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy

Answer	Yes
Document Name	

Comment

Entities currently have several agencies, each with their own form, to report to in the event of a Cyber Security Incident. Many states now also require reporting with their own form, and more states are following suit. The SDT should consider coordinating with other agencies, such as the DoE, to consolidate to a single form. Unique forms for each agency introduce considerable risk for meeting the reporting deadline.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

We suggest the following changes to the format and content of the form:

Attachment 1 appears to require the first and last names of the primary point of contact, but the form never requests the name of the Responsible Entity. We would suggest including a box that asks for this information.

Additionally, the “Required Attribute Information” fields should parallel the order in the Standard for consistency. “Attack Vector” should be listed second, and “Functional Impact” should be listed first.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

No Comment

Likes 0	
Dislikes 0	

Response

Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6

Answer	Yes
Document Name	
Comment	
Recommend Required Attribute Information should have more specificity. Expect the industry will want to see trending over time. Does the Entity still need to submit an EOP-004 or 417 in addition to the Attachment 1? Concerns regarding information protection when submitting Attachment 1	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
However, please reference BPA’s response to Question 1 regarding “attempt.”	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	

Comment
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Douglas Johnson - American Transmission Company, LLC - 1	
Answer	
Document Name	

Comment
Abstain. ATC agrees with the content of Attachment 1 will meet FERC directives, and understands the SDT labored about how to keep it both simple and useful. ATC believes there may be opportunity to share better information and further minimize risk and exposure to the Bulk Electric System if this included some mechanism for timely and secure sharing of additional pertinent (and optional) details as like indicators of compromise, detection mechanism, and exploits used/vulnerabilities exploited. ATC requests the SDT reconsider whether the use of Attachment 1 must be a requirement.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	

Comment
Texas RE seeks clarification on whether or not Attachment 1 is required for reporting. Requirement Part 4.2 does not explicit say entities must submit Attachment 1 for all notifications. Texas RE recommends adding an additional comment box to Attachment 1 for the entity to provide any additional information that does not specifically align to the three attributes.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy does not agree with the use of Attachment 1, as if NERC requires the use of the Attachment for notification, then it should be referenced in the Requirement language. NV Energy would request the SDT revise the language to allow any form of an electronic document/evidence by the notifying entity that includes 1) The functional impact; 2. The attack vector used; and 3. The level of intrusion that was achieved or attempted. This would be in lieu of making Attachment 1 a required submittal.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
See comments of the ISO/RTO Council.	
Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends that “Attachment 1” not be included in any requirement. Incident reporting should follow published methods already defined by the DHS Federal Incident Notification Guidelines. Only one reporting form should be used for all incident reporting, including CIP-008 and EOP-004. Multiple different forms (CIP-008 Attachments 1 and 2; EOP-004 OE-417 and Attachment 2, etc.) create confusion and provide opportunities for errors and omissions.

Reclamation also recommends CIP-008 Requirement R4 Parts 4.2 and 4.4 be modified to include “or in a manner permitted by the E-ISAC” as an additional acceptable E-ISAC notification mechanism. The language requiring submission of Attachment 1 within 5 days should be withdrawn because it potentially creates an unnecessary paperwork burden on entities, especially if the E-ISAC provides a more efficient mechanism to maintain this information in the future (e.g. a webpage, etc.).

Additionally, Reclamation recommends Requirement R4 Parts 4.2 and 4.4 include an exception for CIP Exceptional Circumstances and for situations when E-ISAC is unable to accept notifications.

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 Company disagrees with the proposed options for reporting, and recommends the SDT focus on the “what” and not the “how” of the requirements. For example, the Standard does not currently allow for advancements in automated data processing where web reporting services could be used to allow for automation of reporting and the updating of submitted information.

In FERC Order 848, FERC states[1],

“We also support the adoption of an online reporting tool to streamline reporting and reduce burdens on responsible entities”

Southern Company agrees with this statement as well as FERCs assertion that a Section 1600 data request is inappropriate for this type of information reporting. Aligned with this belief, Southern Company contends the ultimate goal of “attempted incident reporting” is to share indicators of compromise attempts at machine speed in the future. We do not agree with prescribing that this be must done by a particular form filled in by humans. While this

may work in the short term, the future goal should be to move beyond this manual process as technology allows, making the requirement obsolete due to its overly prescriptive method.

Additionally, we affirm that the standard should be results-based and not prescribe a manual form be used. If something needs to be changed on the form in the future, NERC will need to stand up a SDT, ballot the changes with industry, and file with FERC. Experience shows that it will take a year or more to make any change to the form. The SDT should consider that any guidance on "how" the required elements may be reported is better covered in Implementation Guidance. The recipients of the data may desire to design web interfaces or web services in the future for the submission of this data. If E-ISAC or ICS-CERT design something within their portal for ease of submission and ingestion of this data, we believe the proposed requirement to use a form is unwarranted and counterproductive.

[1] FERC Order No. 848, *Cyber Security Incident Reporting Reliability Standards* ¶ 61,033 (2018), Docket No. RM18-2-00, Page 58, Section 91

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Would strongly prefer to see it merged with OE-417.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

The approach to reporting should be related to a reporting process agreed to by both E-ISAC/ICS-CERT as opposed to use of a form. We should try to avoid specifying technology versus outcomes. Should this simply be left with notification to groups as opposed to specifying means – given an incident may remove one or more means for reporting (i.e. internet access disconnect or similar measures during an incident)?

Regarding the form in Attachment 1, this could instead be specification of a schema for reporting that could be incorporated into a portal or similar reporting process as determined by E-ISAC (and/or ICS-CERT). The standard should be technology independent as much as possible. The standard

should speak to responsible entity concerns regarding the information sharing classification of this sort of report for E-ISAC and ICS-CERT (TLP of some sort, PCII, how does FOIA get involved?).

Regarding contact information required for the form in Attachment 1, there should be provision for an alternate contact to support operational contacts. The standard should clarify whether this is meant to be a compliance contact or an operational (cyber) contact. The standard should address expectations for access to a contact (24 by 7, next business day, etc.) by E-ISAC/ICS-CERT during an investigation so entities can select appropriate contacts and ensure responsible parties provide reasonable response in such cases

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC

Answer	No
Document Name	

Comment

We recommend “Required Attribute Information” should have more specificity. Expect the industry will want to see trending.

Does the Entity still need to submit an EOP-004 or 417?

What about information protection when submitting?

We recommend that directions to filling out Attachment 1 should point to Attachment 2.

We recommend that this form and the means to submit should be more technically agnostic.

Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

Overall, the reporting form provided in Attachment 1 is good and aligns with FERCs Order. However, the CIP-008 reporting requirements need to be reviewed in concert with EOP-004 and OE-417. The overlap in these requirements creates multiple reporting thresholds and multiple dissimilar reporting timeframes and forms. This overlap will create confusion and will be burdensome for entities to manage. There will also be inconsistencies between what is reported by entities on the OE-417 form versus CIP-008 Attachment 1.

To address this overlap, SCE&G recommends EOP-004 be revised to omit CIP-008 Applicable Systems, since these assets are effectively be covered by the CIP-008 Standard. NERC should work with the DOE to develop a process to share information provided by entities in CIP-008 reports.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We agree with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

APPA believes that the new form should fit with other forms and existing reporting requirements to avoid duplication. The proposed form does not tie to the reporting content specified in EOP-004-4 that syncs up with the Department of Energy's OE-417. In addition, the E-ISAC already has a web-based reporting mechanism which could be used to capture this information. The E-ISAC web-based reporting method also solves the concerns about undefined process and encryption requirements.

The proposed form adds a new reporting requirement to notify the ICS-CERT that does not have its own reporting structure. ICS-CERT refers enities to the NCCIC for reporting (including the US-CERT). The current notification form on the E-ISAC portal provided Entities with an option to notify a number of different organizations. An option would be to incorporate any additional reporting requirements via the E-ISAC portal. Companies, especially smaller utilities should not be encumbered with duplicative portals, email addresses and telephone numbers to track for reporting.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

The requirement (R4.4) to use Attachment 1 for reporting should be eliminated. Use of the form is a cumbersome manual process that will put unnecessary constraints on the ability of entities to report. This is likely to be especially true in the case of Reportable Attempted Cyber Security Incident which, depending on interpretation, could number in the hundreds per day. No one has a good idea of how many reports will be necessary now or, especially, in the future. Requiring use of Attachment 1 would put an administrative burden on reporting entities and hamper the ability of entities, E-ISAC and ICS-CERT to develop automated reporting tools and processes. The Standard should concentrate on the security objective and not specify how it is met. Attachment 1 could be included in a guidance document as an optional way of complying. Alternatively, use of the form could be a recommendation from E-ISAC and ICS-CERT.

Likes 0	
Dislikes 0	

Response

Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

The standard is not clear on how to report an incident that was an attempt to compromise or a compromise to the PSP. The standard clearly states not to use Attachment 1 for this. It's easier for Registered Entities to use one form for all Reportable Cyber Security Incidents. Recommend that Attachment 1 include information for reporting attempts to a PSP.

Likes 0	
Dislikes 0	
Response	
Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	No
Document Name	
Comment	

Tacoma Power agrees with APPA comments:

"APPA believes that the new form should fit with other forms and existing reporting requirements to avoid duplication. The proposed form does not tie to the reporting content specified in EOP-004-4 that syncs up with the Department of Energy's OE-417. In addition, the E-ISAC already has a web-based reporting mechanism which could be used to capture this information. The E-ISAC web-based reporting method also solves the concerns about undefined process and encryption requirements.

The proposed form adds a new reporting requirement to notify the ICS-CERT that does not have its own reporting structure. ICS-CERT refers enities to the NCCIC for reporting (including the US-CERT). The current notification form on the E-ISAC portal provides entities with an option to notify a number of different organizations. An option could be to incorporate any additional reporting requirements via the E-ISAC portal. Companies, especially smaller utilities, should not be encumbered with duplicative portals, email addresses, and telephone numbers to track for reporting."

Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	

APPA appreciates the SDT's efforts to ensure consistent reporting in compliance with FERC Order 848 and supports the identified information contained in the Attachment 1 form; however, we have concerns about requiring the use of the Attachment 1 form in Requirement R4, Parts 4.2 and 4.4. Required use would unnecessarily constrain entities in the method and manner in which they convey qualifying Cyber Security Incident information today to organizations such as E-ISAC and ICS-CERT. Moreover, duplication or restating existing reporting is not efficient and obligating the industry to use the proposed form would obstruct the creation of more efficient reporting mechansims. Also, use of the proposed form would be complicated by unintentional omissions or mistakes that could result in compliance violations, leading to inefficient use of resources by both entities and the ERO. Because of these concerns, APPA recommends that Attachment 1 not be required, but rather be provided as an example or suggested method for submitting Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents.

The requirement (R4.4) to use Attachment 1 for reporting is a cumbersome manual process that will put unnecessary constraints on the ability of entities to report. Based on current reporting, Reportable Attempted Cyber Security Incidents which, depending on the definition and its interpretation,

could be hundreds per day and could increase in the future. Requiring use of Attachment 1 would put an administrative burden on reporting entities and as mentioned above, constrain complying entities, E-ISAC, and ICS-CERT from developing better automated reporting tools and processes. APPA recommends that the Standard focus on the security objective without specifying a specific form. Attachment 1 can best be provided as a guidance document, or as something that complements existing E-ISAC and ICS-CERT reporting.

APPA believes that any new form (required or not) should fit with other forms and existing reporting requirements to avoid duplication. The proposed form does not tie to the reporting content specified in EOP-004-4 that syncs up with the Department of Energy's OE-417. In addition, the E-ISAC already has a web-based reporting mechanism which could be used to capture this information. The E-ISAC web-based reporting method also solves the concerns about undefined process and encryption requirements.

The proposed form adds a new reporting requirement to notify the ICS-CERT that does not have its own reporting structure. ICS-CERT refers enities to the NCCIC for reporting (including the US-CERT). The current notification form on the E-ISAC portal provides entities with an option to notify a number of different organizations. An option could be to incorporate any additional reporting requirements via the E-ISAC portal. Companies, especially smaller utilities, should not be encumbered with duplicative portals, email addresses, and telephone numbers to track for reporting.

Likes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb

Answer	No
Document Name	

Comment

The companies have three suggestions:

1. Add “BES Cyber System Information” to the Attachment 1 header and language addressing information protection;
2. Add language to the form that provides flexibility to E-ISAC and ICS-CERT to develop an alternative format for submission; and
3. Add an “incident identifier” field.

1. Adding “BES Cyber System Information” (BCSI) to Header

The companies recommend adding “BES Cyber System Information” to the Attachment 1 header and the following statement in the body of the form:

“The information contained in Attachment 1 may include BES Cyber System Information (BCSI) and FERC defined Critical energy infrastructure information (CEII) (18 C.F.R. § 388.113). Registered Entities shall protect disclosure of Attachment 1 information except as required by FERC Order 848.

Disclosure of information contained in Attachment 1 is with limitation and shall not be disclosed except to E-ISAC and ICS-CERT in the manner as set forth under [Add citation to FERC Order 848].”

Background

The information included on the form will fall under the NERC Glossary Term, *BES Cyber System Information;* specifically, Attack Vector, Functional Impact, and Level of Intrusion.

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

Also, the nature of the Attachment 1 information easily falls within the FERC definition of Critical energy infrastructure information (CEII).

"**Critical energy infrastructure information** means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:

[…]

(ii) Could be useful to a person in planning an attack on critical infrastructure;

[…]"

(Excerpt, 18 C.F.R. § 388.113 (c)(2))

In addition, the case can be made there will be instances the data reported will not explicitly fall within the BCSI Glossary Term; however, we consider information regarding the volume of unsuccessful attacks "could be useful to a person in planning an attack on critical infrastructure" even in the case the information is non BCSI.

Bad actors are informed of potential vulnerabilities by a high volume of attacks, that the vulnerability may be a rich target to breach security. Of equal concern is an attacker's strategy being informed by a low volume of attempts, suggesting to the attacker to look for viable vulnerabilities elsewhere.

Either way, any information that informs an attacker's strategy "…could pose a security threat to the BES Cyber System…" and we believe treating Attachment 1 as BCSI or CEII, for that matter, while not perfect solutions, will better protect the reliability of the BES.

2. Alternative Format Language

The companies take the position that E-ISAC and ICS-CERT should have flexibility in the format of how the information is received by these organizations. It is our expectation E-ISAC and ICS-CERT would consult and agree on the same format for submitting data.

Attachment 1 is incorporated by reference into the Requirements and will be treated as required under the Standard. Since this is the case, flexibility in the format of the submission would lend itself to efficiency by not requiring changes to Attachment 1 to go through the Standards Drafting Process every time changes are needed.

The companies believe the intent of Attachment 1 and Order 848 us to provide clarity as to **what** information should be submitted to E-ISAC and ICS-CERT, not the format as to **how** it's submitted.

Accepting that as the case, we offer the following statement to be included on the form and / or other enforceable section of the Standard as the SDT may see fit:

Attachment 1 represents the required data, if known, for submission to E-ISAC and ICS-CERT. The format of the form, not the specified content, may be modified by agreement of E-ISAC and ICS-CERT.

3. Incident Identifier Field

The companies would not normally make a “process” suggestion, but should Attachment 1 be approved without an option for flexibility as to format, we recommend adding a field that provides an incident identifier for each submission so to easily identify initial and any subsequent reporting as relating to the same incident.

Though we believe E-ISAC and ICS-CERT would provide an incident identifier for each submission, we did not want to make that assumption and offer it to the SDT for consideration on Attachment 1.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant

Answer	No
Document Name	

Comment

Luminant is concerned with the use of Attachment 1. Luminant understands that the SDT did not feel it was feasible to modify the OE-417, but Luminant thinks this is the only reasonable path forward. Having to complete two separate forms with significant overlap related to cybersecurity incidents but different overall objectives forces entities to focus on reporting an incident over responding to an incident. Additionally, the OE-417 has clear provisions regarding confidential information, FOIA and CEII such that an entity understands how its contents are protected and shared. The standard as currently written does not include any provisions regarding the protection of its contents or the circumstances under which it can be publicly or privately disclosed. Given the media’s inclination for hyperbole regarding cybersecurity and the energy sector, clear provisions and strong protections are critical. At the very least, Attachment 1 should be stamped CEII within the standard itself; however, Luminant is opposed to using Attachment 1 at all and prefers the SDT pursue modifications to the OE-417. Additionally, while NERC and the E-ISAC are required to follow CEII handling and protections, we are uncertain whether ICS-CERT as a division of DHS has the same constraints.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Agree that there should be minimum requirements for submission of reports and with the proposed form, but would

The suggested FORM, Attachment 1, should not be required in it's present form. Request that you add check boxes: (e.g., unknown, EACMS) rather than just a narrative piece that meet with the instructions/requirements.

Entity should be allowed to submit in ANY format, as long as the report contains the same specified fields of information. Standards **should not be technology-dependent**. Forms tend to be revised over time**. Having the Attachment 1 form as part of the standard would require another SAR to tweak the form**.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No
Document Name	

Comment

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - 1,3,5 - NA - Not Applicable

Answer	No
Document Name	

Comment

EEI supports SDT efforts to ensure consistent reporting in conformance with FERC Order 848 and supports the identified information contained in the Attachment 1 form; however, we are concerned about requiring the use of the Attachment 1 form in Requirement R4, Parts 4.2 and 4.4. Such an obligation would unnecessarily constrain entities in the method and manner in which they convey qualifying Cyber Security Incident information to the E-ISAC and ICS-CERT. Over time more automated and efficient methods of submitting this information may be created. Obligating the industry to use the proposed form would create a barrier to using such new, more efficient reporting mechansims. Moreover, any unintentional omission or mistake while using the proposed form could result in compliance violations, leading to inefficient use of resources by both entities and the ERO. To resolve this concern, EEI recommends that Attachment 1 be provided as an example or suggested method for submitting Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents.

Likes 0	
Dislikes 0	

Response

Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	No
Document Name	
Comment	
Based on AZPS's recommended language in R4.4, we recommend changing the form to include an option for "complete" and remove the option for "update".	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	
Should not include "Reportable Attempted Cybersecurity Incident."	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with the following comments submitted by APPA: APPA believes that the new form should fit with other forms and existing reporting requirements to avoid duplication. The proposed form does not tie to the reporting content specified in EOP-004-4 that syncs up with the Department of Energy's OE-417. In addition, the E-ISAC already has a web-based	

reporting mechanism which could be used to capture this information. The E-ISAC web-based reporting method also solves the concerns about undefined process and encryption requirements.

The proposed form adds a new reporting requirement to notify the ICS-CERT that does not have its own reporting structure. ICS-CERT refers enities to the NCCIC for reporting (including the US-CERT). The current notification form on the E-ISAC portal provides entities with an option to notify a number of different organizations. An option could be to incorporate any additional reporting requirements via the E-ISAC portal. Companies, especially smaller utilities, should not be encumbered with duplicative portals, email addresses, and telephone numbers to track for reporting

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

Follow-on reporting in Requirement R4.4 requires repeated reporting until all attributes of the event are known, but determination of attack vector, impact, or level of intrusion may be impossible to ascertain during or after the event. A qualifier needs to be added to Requirement R4.4 to only require reporting of attributes that can be determined.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

See comments from the MRO NERC Standards Review Forum.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No

Document Name	
Comment	

We recommend “Required Attribute Information” should have more specificity. Expect the industry will want to see trending.

Does the Entity still need to submit an EOP-004 or 417?

What about information protection when submitting?

We recommend that directions to filling out Attachment 1 should point to Attachment 2.

We recommend that this form and the means to submit should be more technically agnostic

Likes 0	
Dislikes 0	
Response	
Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	No
Document Name	
Comment	

As noted in question 1

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

Utility Services agrees with APPA's comments.

Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

The addition of specific information collection data points would be helpful in more quickly analyzing and providing useful information to the industry.

Additional information to consider collecting:

- Entity's Name, NERC ID and registered function(s)
- Entity's internal tracking number (e.g. IRT Case #, Change Record, etc.)
- Timestamps including the timezone the report is being made from
    - Date/time of report
    - Date/time incident start
    - Date/timeincident detected
- Discovery Method (malware detection, operator reported suspicious activity, etc.)
- Identification of external organizations that have been notified or engaged (e.g. law enforcement, etc.)
- Define and provide common "Functional Impact" categories (critical and non-critical) as part of the reporting form for consistent reporting purposes (e.g. No impact | Minimal Impact | Significant Impact | Denial of Critical Services/Loss of Control, Destruction Impact)
- Define and provide common "Attack Vectors" or use known taxonomy as part of the reporting form for consistent reporting purposes (e.g. Unknown, Attrition, Web, e-mail/Phising, External/Removable Media, Web/IRA, Improper usage, loss or theft of equipment)

Likes 0	
Dislikes 0	
Response	

Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	No
Document Name	
Comment	

While we generally agree with the content and use of Attachment 1, we would ask that NERC and the SDT consider coordinating with E-ISAC and ICS-CERT to implement an electronic version of the form for ease of initial reporting, updating, and tracking by the Responsible Entity (RE). Furthermore, if upon submission, the form could automatically route the data to both agencies, that would save the RE the undue burden of submitting twice and potentially encountering discrepancies between the two agencies during initial and updated submissions. If automation is not possible, consider adding a check box on the form indicating that E-ISAC needs to forward the report to ICS-CERT. It is our understanding that E-ISAC already works with National Cybersecurity and Communications Integration Center (NCCIC) of which ICS-CERT is one branch. This would cover the RE's responsibility to

report to both agencies when necessary, but ensures E-ISAC and ICS-CERT are coordinating any response. The electronic submission should incorporate encryption or other security measures to ensure the information remains confidential.

Also, it is unclear whether updates to the form can only include the required attribute that is being updated and all other attributes can be left blank, or if it is intended that the RE re-submit attribute information which has not changed since the last update. If it is intended to be resubmitted, would an RE check the “initial” box for that attribute, or “update” even if there was no update to that specific attribute? Depending on the intent, we ask that the SDT consider whether it is redundant to include an “initial” and “update” checkbox for each individual attribute when it is already documented in the “Reporting Category” section above. If it isn’t redundant then consider a “no update” checkbox to be added to each attribute.

In addition, in the event that the RE has reported a Reportable Attempted Cyber Security Incident, but later through additional investigation determines it was a false positive, the form does not appear to have a way to retract or withdraw the report.

Finally, in Attachment 2, under the guidance for each required attribute, it states “If not know, specify ‘unknown’ in the field.” It is unclear if “unknown” can be acceptable as a final report answer.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3

Answer	No
Document Name	

Comment

Automation and JSON or XML formats should be supported for reporting events. Completing a form manually will lead to errors that affect data accuracy, which is crucial for analysis and trending.

Likes 0	
Dislikes 0	

Response

Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC

Answer	No
Document Name	

Comment

WAPA does not believe that “Attachment 1” should be included in any language of the requirement. Reporting of an incident should follow published methods already defined by the US-CERT Federal Incident Notification Guidelines. The inclusion of Attachment 1 requires duplication in effort and could require entities to provide two separate forms of reporting. The US-CERT Incident Reporting System is already established and provides the necessary information and capability to report incidents.

ALSO: Reclamation recommends one reporting form be used for all incident reporting, including CIP-008, EOP-004. Multiple different forms (CIP-008 Attachments 1 and 2; EOP-004 OE-417 and Attachment 2, etc.) create confusion and provide opportunities for errors and omissions.

Reclamation also recommends Requirement 4 Part 4.2 and 4.4 be modified to include “or in a manner permitted by the E-ISAC” as an additional acceptable E-ISAC notification mechanism. The language requiring submission of Attachment 1 within 5 days should be withdrawn because it potentially creates an unnecessary paperwork burden on entities, especially if the E-ISAC provides a more efficient mechanism to maintain this information in the future (e.g. a webpage, etc.).

Reclamation also recommends Requirement 4 Parts 4.2 and 4.4 include an exception for CIP Exceptional Circumstances and for situations when E-ISAC is unable to accept notifications.

Reclamation also recommends Requirement 4 Part 4.4 specify the allowable method(s) for submitting Attachment 1 updates.

Likes 0	
Dislikes 0	

Response

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	Attachment 1A.DOCX

Comment

Recommend redesign of Attachment 1 to align with comments for updated language of proposed modified term *Reportable Cyber Security Incident* and proposed new term *Reportable Attempted Cyber Security Incident*. See Attachment 1A.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	No
Document Name	

Comment

WEC Energy Group supports SDT efforts to ensure consistent reporting in conformance with FERC Order 848 and supports the identified information contained in the Attachment 1 form; however, we are concerned about requiring the use of the Attachment 1 form in Requirement R4, Parts 4.2 and 4.4. Such an obligation would unnecessarily constrain entities in the method and manner in which they convey qualifying Cyber Security Incident information to the E-ISAC and ICS-CERT. Over time more automated and efficient methods of submitting this information may be created. Obligating the industry to use the proposed form would create a barrier to using such new, more efficient reporting mechansims. Moreover, any unintentional omission or mistake while using the proposed form could result in compliance

violations, leading to inefficient use of resources by both entities and the ERO. To resolve this concern, WEC Energy Group recommends that Attachment 1 be provided as an example or suggested method for submitting Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
We do not believe that the reporting forms should be attachments to the standard, but rather should follow the BAL-003 model with FRS Forms 1 and 2. Using the attachment approach will require a revision to the standard in order to make minor information sharing improvements needed by the E-ISAC.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Besides meeting CIP-008 reporting requirement, for the same event, an entity may also have EOP-004 and OE-417 reporting requirements to fulfill. These standards/regulation have different reporting requirements and reporting timeline. Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format. We recommend that an entity use CIP-008-6 proposed reporting timeline.	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	No
Document Name	

Comment
I do not believe that the reporting forms should be attachments to the standard, but rather should follow the BAL-003 model with FRS Forms 1 and 2. Using the attachment approach will require a revision to the standard in order to make minor information sharing improvements needed by the E-ISAC.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	

Comment
We agree with the content of Attachment 1, but entities should be allowed to submit reports in any format as long as the report contains the same specified fields of information. Standards should not be technology-dependent. Forms tend to be revised over time. Having the Attachment 1 form as part of the standard would require another SAR to tweak the form.

Likes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	

Comment
Besides meeting CIP-008 reporting requirement, for the same event, an entity may also have EOP-004 and OE-417 reporting requirements to fulfill. These standards/regulation have different reporting requirements and reporting timeline. Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format. We recommend that an entity use CIP-008-6 proposed reporting timeline.

Likes 0	
Dislikes 0	

Response

Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	No

Document Name	
Comment	
No discussion of overlap or hierarchy with regards to OE-417.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	No
Document Name	
Comment	
No discussion of overlap or hierarchy with regards to the OE-417.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
No discussion of overlap or hierarchy with regards to the OE-417.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SRP agrees with the form as an industry template for consistency. If reporting attributes change within 5 days adds administration burden of having the template attachment completed. SRP recommends an adjustment to "when the investigation is complete" so an investigation with all the facts are presented.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The content seems to be sufficient, except the definition of “Reportable Attempted Cyber Security Incident” is still unclear. What does it mean to attempt? What includes an attempt?

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Entities should not be required to use a specific form through reference in a Requirement. Using a static form could preclude entities from providing appropriate information as each actual or attempted cyber incident is different, requiring specific information to be provided to be of value, and the cyber landscape continues to evolve, which may require different information to be provided in the future. The current form would be required to be used 'as is' unless the Standard was modified. An additional concern is that any omissions or mistakes in using the form could result in unecessary compliance activities, leading to an inefficient use of resources by both entities and the ERO. Dominion Energy is of the opinion that proposed Attachment 1 should either be removed or be provided only as an example and not a requirement.

Likes 1	Massachusetts Municipal Wholesale Electric Company, 5, Gordon David
Dislikes 0	

Response

5. Do you agree with the required methods of notification proposed by the SDT in Requirement R4, Part 4.2? If no, please explain and provide comments.

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

NV Energy believes the listed methods of notification are sufficient. However, there is redundancy in the language, "electronic communication" and "email", as email is a form of electronic communication. If the term "electronic communication" is preparation for an online submittal portal for E-ISAC and ICS-CERT then NV Energy believes the language is sufficient.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP agrees

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3

Answer	Yes
Document Name	

Comment

AEP supports the methods of notification as proposed by the SDT in R4 Part 4.2. In addition we would support the idea of reporting to the E-ISAC who would then act as a conduit to other governmental agencies on behalf of the reporting entity. AEP feels this would streamline the reporting process, lessen the reporting burden on members and ensure all necessary agencies are informed appropriately.

Likes 0	

Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
NO comment	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA recommends that the drafting team add the following language to the end of the first bullet under 4.2 Requirements: “, or equivalent web for if offered by the E-ISAC”.	
Likes 0	
Dislikes 0	
Response	

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
We recommend that the drafting team add the following language to the end of the first bullet under 4.2 Requirements: “, or equivalent web for if offered by the E-ISAC”.	
Likes 0	
Dislikes 0	
Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	Yes
Document Name	
Comment	
GSOC recommends that the drafting team add the following language to the end of the first bullet under 4.2 Requirements: “, or equivalent web for if offered by the E-ISAC”.	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
R4 VSL implies a preference for the use of the form for notification. If there is an order of preference for these methods, it should be clearly stated in the standard.	
Likes 0	
Dislikes 0	
Response	

Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
ATC requests consideration of adding a ‘catch all’ in an attempt to accomplish a technology agnostic approach, and ‘future proof’ it enough so it can adapt/scale as E-ISAC and ICS-CERT processes mature and change without requiring modifications to the Standard.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
NC	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1, Group Name Exelon Utilities	

Answer	Yes
Document Name	
Comment	
Exelon supports the methods of notification, but asks the standard drafting team to include a note in the form to request receiving entities confirm receipt or provide another method of ensuring entities receive such a confirmation.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Again, would rather not see a separate form created.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
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	
Answer	Yes
Document Name	
Comment	
Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
See comments of the ISO/RTO Council. ERCOT also adds that it has concerns with the suggestion to email the form that may contain sensitive information. A secure submission means should be used or encrypted email.	

Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Reclamation recommends reporting requirements be limited to a single destination and not duplicated between E-ISAC and DHS. Establishing communication between those organizations is not the responsibility of the registered entity. The DHS Incident Reporting System is already established and provides the necessary information and capability to report incidents.

Reclamation also recommends the SDT clarify what method of transmission is meant by “electronic submission of Attachment 1” (e.g., facsimile, web-form, etc.). Requirement R4 Part 4.4 should specify the allowable method(s) for submitting Attachment 1 updates (e.g., electronic submission, facsimile, email, etc.).

Requirement R4 Part 4.2 should be changed

from:

Responsible Entities shall use one of the following methods for initial notification:

Electronic submission of Attachment 1;

Phone; or

Email.

to:

Responsible Entities shall submit initial notification in a manner permitted by the E-ISAC, including electronic submittal, phone, or email.

Finally, Reclamation recommends Requirement R4 not require entities to notify the ICS-CERT. Replace “ICS-CERT” with the “U.S. Department of Homeland Security” instead of any specific CERT entity within DHS.

Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
As discussed in the previous question, Dominion Energy is of the opinion that a static form should not be used for this type of reporting and requiring Attachment 1 in both the Requirements and Measures is inappropriate. While certain information should continue to be required, the methods of notification need to remain flexible.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	No
Document Name	
Comment	
Revise “Electronic submission of Attachment 1” to state “Electronic submission with the specified fields of information identified in Attachment 1 to the extent known.” Remove the email option. It is redundant. Email is a form of electronic submission.	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	No
Document Name	
Comment	
Reporting requirements should be limited to a single destination and not duplicated between E-ISAC and ICS Cert. Establishing communication between those organizations should occur to lessen the reporting obligations of entities.	
Likes 0	
Dislikes 0	
Response	

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	
Reporting requirements should be limited to a single destination and not duplicated between E-ISAC and ICS Cert. Establishing communication between those organizations should occur to lessen the reporting obligations of entities.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	No
Document Name	
Comment	
Please note WEC Energy Group concerns regarding Attachment 1 as described in our response to question 4.	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	No
Document Name	
Comment	
We agree with the required methods, but please describe how to make an electronic submission.	
Likes 0	
Dislikes 0	
Response	
Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	No

Document Name	
Comment	

Reporting requirements should be limited to a single destination and not duplicated between E-ISAC and ICS Cert. Establishing communication between those organizations is not the responsibility of the registered entity. Additionally the US-CERT Incident Reporting System is already established and provides the necessary information and capability to report incidents. ALSO: Reclamation recommends the SDT clarify what method of transmission is meant by “electronic submission of Attachment 1” (e.g., facsimile, web-form, etc.).

Requirement 4.2 should be modified to include “or in a manner permitted by the E-ISAC” as an additional acceptable E-ISAC notification mechanism.

Likes 0	
Dislikes 0	
Response	

Tim Womack - Puget Sound Energy, Inc. - 3

Answer	No
Document Name	
Comment	

Submittal of the manually completed form is inefficient. A better solution, less prone to error is submittal of data in JSON or XML format.
Submittal via plan text email or uploading to an unsecure web site does not provide sufficient security for BCSI and other sensitive, proprietary data. Secure transfer is needed.
The current proposal to submit the same data to two organizations is inefficient and redundant.
A more efficient, secure means of notification would be via an automated solution to a single secure web site

Likes 0	
Dislikes 0	
Response	

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

Answer	No
Document Name	
Comment	

We generally agree with the required methods outlined in R4.2, with a few caveats:

1. We believe there should only be one report necessary (and not two separate reports for E-ISAC and ICS-CERT). See previous comment for #4 regarding form modification to indicate that E-ISAC needs to forward the information to ICS-CERT.

2. It does not appear possible to submit R4.4 notification via phone (due to the use of the word “submission”). If this is not a feasible option for R4.4, it should be specified in R4.4 what notification methods are allowable. The usage of phone as a method in general should be reconsidered for practicality.

3. While electronic submission is one of the methods, we do not yet see instructions for how or where to execute this type of submission. Further guidance on electronic submissions must be provided.

4. Consider adding CIP Exceptional Circumstance exception verbiage to the second paragraph of R4.2 and split out the “without attribute” clause to be a separate sentence for clarity. This proposed modification would read “*If Attachment 1 was not submitted for initial notification, it must be submitted within 5 calendar days, except under CIP Exceptional Circumstances. Initial notification may be submitted without attribute information if undetermined at the time of submittal*.”

5. Consider moving the second paragraph of R4.2 to R4.4 for clarity.

6. R4.3 appears to be part of R4.2 and is a sentence fragment, which is inconsistent with the way other requirements are written. Consider modifications to correct inconsistencies.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

Utility Services agrees with APPA's comments.

Likes 0	
Dislikes 0	

Response

Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6

Answer	No
Document Name	

Comment

Agree with NPCC comments

Likes 0	
Dislikes 0	

Response
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman
Answer	No
Document Name	
Comment
See comments from the MRO NERC Standards Review Forum.
Likes 0	
Dislikes 0	
Response
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE
Answer	No
Document Name	
Comment
There is a conflict between required reporting of [successful] attack vectors and safe handling of BES Cyber System Information (BCSI), or information that could be used to gain unauthorized access or pose a security threat to a BES Cyber System. CenterPoint Energy suggests that the details of how E-ISAC and/or ICS-CERT will provide verifiable records of phone reports be outlined in the requirement or guidance. Assurances that phone conversations with E-ISAC and/or ICS-CERT are confidential should also be noted in the components of this modification. CenterPoint Energy requests provisions for the security and confidentiality of phone calls, email, and electronic submissions. The SDT may consider outlining the secure methods in Implementation Guidance. For example, ICS-CERT has published a PGP public key for secure email communications. E-ISAC could consider similar secure measures. Responsible Entities need a means and assurance for the secure and confidential transfer, storage, and use of BCSI.
Likes 0	
Dislikes 0	
Response
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA
Answer	No
Document Name	
Comment

FMPA agrees with the following comments submitted by APPA:

The required methods of notification include the ICS-CERT, which does not have an official reporting structure. While we recognize that FERC indicated that the Cyber Security Incident should be sent to the E-ISAC and ICS-CERT, we believe that the actual required notifications should meet current Department of Homeland Security (DHS) practices. As a DHS agency, the National Cybersecurity and Communications Integration Center (NCCIC) has protocols for reporting to ICS-CERT that could be substituted.

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - 1,3,5 - NA - Not Applicable

Answer	No
Document Name	

Comment

Please note EEI concerns regarding Attachment 1 as described in our response to question 4.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No
Document Name	

Comment

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment
Hard NO on submitting our reports to E-ISAC, Homeland Security & ICS-Cert separately! That would be onerous during the response to a cyber incident. Resources are needed to mitigate the incident and communicate to management. They should establish their own internal reporting much as the DOE does with the OE-417. Revise the term: 'Electronic submission,' reporting medias are: phone, email, fax…**all are forms of 'electronic' submissions**. Revise Standard language from, "Electronic submission of Attachment 1" and state, "Electronic submission with the specified fields of information identified in Attachment 1 to the extent known." **Remove the email option**. It is redundant. Email is a form of electronic submission. Regisered entities should only be required to report ONLY to E-ISAC, then the burden is on E-ISAC to forward to ICS-CERT and are self accountable, thus completing a truly confidential reporting system. This would serve to protect annionimity, and lessens the burden on the industry for reporting, thus retaining continued continuity in the information being reported. Dual reporting and dual updtates and tracking opens up the industry and the nature of the Standard, to miscommunications.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant	
Answer	No
Document Name	

Comment
Luminant has significant concerns regarding the current notification language. First, the bullets in 4.2 list electronic submission and email as two different methods. We are not aware of any mechanism to electronically submit the incident report to either the E-ISAC or ICS-CERT and therefore would be limited to submitting via email which offers insufficient protection for information of this nature. Second, we are opposed to submitting this information to multiple agencies. At the minimum, we will be required to submit the same form to two separate agencies and a different form to the DOE. This is administratively burdensome and focuses immediate activities on reporting rather than resolving the incident. Additionally, there is opportunity to inadvertently report information inconsistently through Attachment 1 and the OE-417 or for the information submitted to be interpreted inconsistently due to the different focus of the reports. The OE-417 has an elegant submission process that allows entities to submit information through a private and encrypted portal and also allows us to elect to send the submission to E-ISAC automatically. Anything less than this mechanism is a step backward and should be avoided. Perhaps the E-ISAC can implement a similar solution and convince the DOE to give up cybersecurity event reporting through the OE-417 in favor of receiving the E-ISAC submissions. Whatever solution is implemented, it should ensure that entities are not required to submit multiple forms to multiple agencies through multiple mechanisms.

Likes 0	
Dislikes 0	

Response

Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	No
Document Name	
Comment	

Tacoma Power agrees with APPA comments:

"The required methods of notification include the ICS-CERT, which does not have an official reporting structure. While we recognize that FERC indicated that the Cyber Security Incident should be sent to the E-ISAC and ICS-CERT, we believe that the actual required notifications should meet current Department of Homeland Security (DHS) practices. As a DHS agency, the National Cybersecurity and Communications Integration Center (NCCIC) has protocols for reporting to ICS-CERT that could be substituted."

Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	

The flexibility of the options for making an initial report is good. However, entities should not be required to submit Attachment 1 within 5 days. Requiring the use of a manual form for reporting cyber security incidents is an anachronism that will place expensive constraints on the development of more cost-effective tools for timely reporting. Requiring use of the form also reduces opportunities for reporting methodologies that would enhance situational awareness.

Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

The required methods of notification include the ICS-CERT that do not have an official reporting structure. While we recognize that FERC indicated that the Cyber Security Incident should be sent to the E-ISAC and ICS-CERT, we believe that the actual required notifications should meet current

Department of Homeland Security (DHS) practices. DHS agency, the National Cybersecurity and Communications Integration Center (NCCIC) has protocols for reporting to ICS-CERT that could be substituted.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	
We agree with EEI's comments for this question.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
PSEG supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	
Comment	
The standard should not limit the entity to these specific forms of communication, since during an incident, these methods may not be appropriate. In addition, the standard should reflect that such information must be sent using the most secure mechanism available at the time. It may not be advisable	

for an entity to send such information using traditional email. Further, since the standard is requiring that incidents be reported to multiple entities, it may not be appropriate to limit the list of allowed contact methods.

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

Please see the answer to Q4.

Furthermore, Southern Company is concerned with the recommended methods of initial notification. To submit the elements of Attachment 1 via e-mail can potentially expose BCSI and other sensitive information as e-mail is inherently insecure and is plain text at the protocol level by design. Additionally, if the e-mail system has been compromised as part of an event being responded to, this method of reporting could expose information to attackers that can be used to further their agenda. The potential for disclosure of BCSI via e-mail traffic or the risk of having e-mail traffic sniffed in route makes this a prohibitive option for use and is counterproductive to reducing risk.

Submission by phone requires those who can submit this information do so from a Company phone that logs and / or records to provide the required evidence of submission, which can be costly and burdensome to entities in the wake of performing actual incident response. If this submission is performed, for example, on a personal cell phone, company personnel could be unknowingly bringing their personal data into scope of the requirements for audit purposes. This represents an undue compliance burden.

Southern reiterates its position that the requirements should focus on the “what” information is required to be reported and focus recommendations for “how” to report that information in Implementation Guidance to avoid requiring cumbersome or risky reporting methods that also severely limits the potential to develop and use an Application Programming Interface (API) for automated information submission.

Likes 0	
Dislikes 0	

Response

6. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R4? If no, please explain and provide comments.

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	Yes
Document Name	

Comment

Yes, however for High VSL, consider adding an additional criteria that includes failure to notify E-ISAC **or** ICS-CERT.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	Yes
Document Name	

Comment

NC

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
See comments from the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
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	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	

Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation does not agree with the High VSL for R4. Recommend changing the High VSL from: The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, but failed to notify or update E-ISAC or ICS-CERT, or their successors, within the timeframes pursuant to Requirement R4, Part 4.3. to: The Responsible Entity notified E-ISAC and DHS, or their successors, but did not accomplish the initial notification within the timeframes included in R4.3. Reclamation also recommends adding the following as a third option to the Moderate VSL: *The Responsible Entity initially notified E-ISAC and DHS, or their successors, within the timeframes included in R4.3 but failed to update E-ISAC or DHS, or their successors, within the timeframe included in R4.4.*	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	

NV Energy believes the VSLs for Requirement R4 are too severe for ultimately, a "reporting requirement". We believe the severe VSL should be removed for this Requirement and moved to High, thus shifting the VSL level for the other possible violations of the Requirement.

Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

See comments of the ISO/RTO Council.

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

VSL language should provide tiered severities that reflect the true severity. As written in the draft Standard, *any* failure to report is automatically a Severe VSL regardless of the circumstances behind the failure.

Also, while it has been stated during the drafting process by the SDT that incorrectly reported information should not represent a violation, the language in the current VSL does not make this intent clear. The R4 Lower VSL currently reads (emphasis added):

*"The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident **and the attributes** within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to submit the form in Attachment 1."*

The inclusion of "and the attributes" appears to indicate that not including the attributes (plural) is a cause for violation.

Southern Company recommends:

"The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the ***known*** attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to submit the form in Attachment 1. (4.4)

OR

The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident and the ***known*** attributes within the timeframes pursuant to Requirement R4, Parts 4.1 and 4.3 but failed to use one of the methods for initial notification pursuant to Requirement R4, Part 4.2."

As stated previously, Southern ultimately feels that using or not using one of the prescribed methods in the current draft should not be cause for a violation if the required information is provided to the required named agencies within the required timeframes. Using a form, or an email, or a phone call, or another more technically secure and sound method should be sufficient to have achieved FERC's directives.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008

Answer	No
Document Name	

Comment

Comments: For consistency, High VSL should contain identical explanatory language as Lower and Moderate VSL.

Ex: High VSL- The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident but failed…"

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

The VSLs as defined are too focused on minor administrative details and will generate needless possible violations. Suggest instead that VSLs focus on having a process defined for reporting cyber incidents that aligns with the definition. With regard to notification methods, in a cyber incident, it is possible that traditional contact mechanisms may not be available, so Registered Entities will need the flexibility to use alternative reporting means.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC	
Answer	No
Document Name	
Comment	

We request clarification. At the time of determination, some attributes may not be known. Should the Entity leave that attributes blank (empty) or explicitly enter “unknown.”

We request clarification. ICS-CERT has its own process. Are Entities expected to add additional answers when submitting to ICS-CERT? If ICS-CERT changes its process, are Entities expected to follow that new CERT process when this Standard has not been updated?

Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3	
Answer	No
Document Name	
Comment	

In our opinion the prescriptive nature and detailed required reporting requirements along with the ambiguity around attempted cyber security incident definition increases the risk of a violation without adding value to stakeholders. Furthermore, the required Attachment 1 form, or other contact methods may not be available within the required reporting timeframes. Ameren recommends flexibility in both required attributes and reporting methods.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	
Should not include “Reportable Attempted Cybersecurity Incident.”	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
There are many issues with the language of the proposed definitions and requirements to be addressed before agreement upon VRFs and VSLs can be reached.	
Likes 0	
Dislikes 0	
Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	No
Document Name	
Comment	
The failure to notify information sharing organizations of an unsuccessful Reportable Attempted Cyber Security Incident should result in a Severe VSL determination. GSOC recommends a Medium VSL determination for this.	
Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment
We request clarification. At the time of determination, some attributes may not be known. Should the Entity leave that attributes blank (empty) or explicitly enter “unknown.” We request clarification. ICS-CERT has its own process. Are Entities expected to add additional answers when submitting to ICS-CERT? If ICS-CERT changes its process, are Entities expected to follow that new CERT process when this Standard has not been updated?

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	

Comment
The failure to notify information sharing organizations of an unsuccessful Reportable Attempted Cyber Security Incident should result in a Severe VSL determination. We recommend a Medium VSL determination for this.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	

Comment
The failure to notify information sharing organizations of an unsuccessful Reportable Attempted Cyber Security Incident should result in a Severe VSL determination. NRECA recommends a Medium VSL determination for this.

Likes 0	

Dislikes 0	
Response	
Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	

Reclamation does not agree with the High VSL for R4. Reclamation recommends rewriting the High VSL as follows:

The Responsible Entity notified E-ISAC and ICS-CERT, or their successors, but did not accomplish the initial notification within the timeframes included in R4.3.

Reclamation also recommends the following be added to the Moderate VSL:

The Responsible Entity initially notified E-ISAC and ICS-CERT, or their successors, within the timeframes included in R4.3 but failed to update E-ISAC or ICS-CERT, or their successors, within the timeframe included in R4.4.

Likes 0	
Dislikes 0	
Response	
Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

Given BC Hydro’s response and comments to Question #1, BC Hydro does not feel it is appropriate to comment on the associated VRF or VSL table elements.

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
BPA believes the Severe VSL should read as follows: The Responsible Entity failed to notify E-ISAC ***and*** ICS-CERT, or their successors, of a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident. (R4)

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	

Comment
Please modify the requirement to be aligned with the EOP-004 and OE-417 reporting requirements and reporting timeline.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	

Comment
Please modify the requirement to be aligned with the EOP-004 and OE-417 reporting requirements and reporting timeline.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
The VSLs focus, in part, on the attributes that are reported. The attributes themselves are somewhat ambiguous and not well defined, so including the attributes in determining the severity (which may lead to monetary penalties for a Responsible Entity) of a failure to report seems to be a poor measurement for compliance.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
The failure to notify information sharing organizations of an unsuccessful Reportable Attempted Cyber Security Incident should not result in a severe penalty.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment
In general, Dominion Energy supports the VRF and VSLs with the exception of the inclusion of the requirement to use Attachement 1. Dominion Energy recommends removing all references to Attachement 1 from the VRF and VSLs.

Likes 0	
Dislikes 0	

Response

7. Do you agree with the 12-month Implementation Plan? If you think an alternate, shorter, or longer implementation time period is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees	
Likes 0	
Dislikes 0	
Response	

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	Yes
Document Name	
Comment	
If the scope of the revisions to this standard doesn't change significantly, 12 months is acceptable.	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
12 months would be adequate, not shorter.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Texas RE inquires as to whether there should be an initial performance date for Requirement Part 2.1. As written, Responsible Entities would not be required to do the first test until within 15 months after the effective date of the standard, or 27 months after the effective date of the government authority's order approving the standard.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
See comments from the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
ATC requests the SDT consider tying the Implementation Plan and the CIP-008-6 Effective Date to the latter of 12 months or the publication of Technical Rationale and Implementation Guidance. For example: Where approval by an applicable governmental authority is required, the standard shall become effective on the latter of the first day of the first calendar quarter that is 12 calendar months after the effective date of the applicable governmental authority's order approving the standard, NERC's publication of Technical Rationale and Implementation Guidance, or as otherwise provided for by the applicable governmental authority.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	Yes
Document Name	
Comment	
The agreement is per the understanding that this STD is further edited before issuance, and is completed correctly – then the timeine is acceptable.	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
NC	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
So long as an entity is in the position of defining attempts and the questions regarding reporting can be productively addressed, 12 months should be sufficient to implement the changes involved in existing programs.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1, Group Name Exelon Utilities	

Answer	Yes
Document Name	
Comment	
No additional comments. .	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Registered Entities who may not already have automated systems in place for alerting, logging, or detection of potential Cyber Security Incidents may need more time than 12 months for implementation of these standard changes.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - 1,3,5 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
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	
Answer	Yes
Document Name	
Comment	
Likes 1	Hydro One Networks, Inc., 1, Farahbakhsh Payam
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	

Response

Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Any implementation timelines can only be evaluated with specific reporting requirements.	
Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month Implementation Plan. This will allow **entities time to determine the effects of the revised** requirements and definitions, develop adequate written processes, and train personnel appropriately.	
Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Seminole prefers an 18-24 month implementation plan in order to implement filtering and notification processes used for alerting of attempted intrusions.	
Likes 0	
Dislikes 0	
Response	

Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
To ensure a successful implementation of the revised standard, we recommend that the revised standard become effective the first day of the first calendar quarter that is **eighteen (18) calendar months** after the effective date of the applicable governmental authority's order approving the standard.	
Likes 0	
Dislikes 0	
Response	

James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
To ensure a successful implementation of the revised standard, we recommend that the revised standard become effective the first day of the first calendar quarter that is **eighteen (18) calendar months** after the effective date of the applicable governmental authority's order approving the standard.	
Likes 0	
Dislikes 0	
Response	

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
Given BC Hydro's response and comments to Question #1, BC Hydro does not feel it is appropriate to comment.	
Likes 0	
Dislikes 0	
Response	
Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	No
Document Name	
Comment	
Reclamation recommends a 24-month Implementation Plan. This will allow entities time to determine the effects of the revised requirements and definitions, develop adequate written processes, and train personnel appropriately.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	
Comment	
The vagueness of the definition of a reportable event makes it difficult for Entities to determine what resources will be needed to review and analyze data, how much automation to implement, etc. Entities may need more than 12 months to secure and implement the additional resources needed. Another consideration is whether the two receiving organizations will ready to receive reports within 12 months of the effective date of the new standard. What assurance that they will be ready can be given?	
Likes 0	

Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

With the additional scrutiny that attempted Cyber Security Incidents will likely require due to the modifications to this standard and associated definitions, Responsible Entities (REs) may consider modifying current network architecture for EACMS and/or Intermediate Systems for Interactive Remote Access which may currently be used for multi-impact BCS (i.e., for High, Medium, and Low impact). Splitting impacts used for each EACMS and IRA solutions may reduce investigation and reporting burden by decreasing the attack surface by taking Lows out of the equation. If this is the chosen path, additional time may be necessary for REs to initiate the supply chain and procurement processes. In which case, an 18-month implementation plan would alleviate this concern.

Additionally, with the upcoming CIP-003-7(8) Transient Cyber Asset and Removable Media malicious code risk mitigation for assets containing low impact BES Cyber Systems, it appears that by the time this CIP-008 modification goes into effect, there will be a much larger scope of cyber assets which will need to be investigated for potential Cyber Security Incidents. The impacts of this expansion may also warrant additional time for REs to adequately assess staffing and resource requirements.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

12 months is a very long period of time for implementation. The information and controls and processes for this standard should already be in place and part of a strong incident response and reporting program. The only addition is updating internal processes to submit the information to EISAC for which 12 months is a very long period of time. This should be achievable in 6 months.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No

Document Name	
Comment	
NRECA recommend a 24 month implementation plan in order to provide entities adequate time to implement filtering and notification processes used for alterting of attempted intrusions.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Utility Services agrees with APPA's comments.	
Likes 0	
Dislikes 0	
Response	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
We recommend a 24 month implementation plan in order to provide entities adequate time to implement filtering and notification processes used for alterting of attempted intrusions.	
Likes 0	
Dislikes 0	
Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	No
Document Name	

Comment
: GSOC recommend a 24 month implementation plan in order to provide entities adequate time to implement filtering and notification processes used for alterting of attempted intrusions.

Likes 0	
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No
Document Name	

Comment
With the proposed definition of a Reportable Attempted Cyber Security Incident, a 12-month implementation is not reasonable. The proposed definition will require an increase in staff resources. Given the technical nature involved with tracking and investigating potential "attempts to compromise," resources are presently limited. Staff would need to be hired and properly trained to implement the processes necessary to meet the requirements. In addition, time is required to research and evaluate tools to be purchased and implemented. A minimal implementation timeframe could result in budgetary constraints or a lack of adequate resources, technology and/or tools.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	

Comment
Without Technical Rationale or Implementation Guidance, entities do not have much guidance regarding classifying attempted incidents. If the standards development timeframe does not allow for specific criteria for determining "attempted," CenterPoint Energy recommends that the implementation plan be extended or postponed until after NERC has performed sufficient pilot studies to publish actionable guidance on what an attempted compromise of an EACMS looks like in comparison to normal operations of an EACMS. If the implementation plan is left as-is, entities will be required to define "attempted" events as they deem appropriate given that not doing so could possibly result in millions of reports per day or year.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy believes an Implmentation Plan of 24 months is more feasible. The proposed changes, particularly the reporting of “attempts” will bring about significant process changes, requiring the re-writing of internal procedures. Also, depending on how “attempt” is defined, the amount of dedicated workers needed to monitor and comb through large amounts of data will increase. Changes in procedures and hiring of additional workers will also require training. With anticipated procedure re-writes and additional hiring and training we feel as though an Implementation Plan of 24 months is necessary.	
Likes 0	
Dislikes 0	
Response	
Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with the following comments submitted by APPA: The current implementation plan will require entities to change their CIP-008, as well as EOP-004, reporting. These administrative changes will require system and software changes and planning for the associated resource commitment. Developing the program, gaining consensus internally, training, and testing will take more than 12 months for most entities. APPA recommends a minimum of 18 months for the Implementation Plan	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	No
Document Name	
Comment	

Changes to the standards require Responsible Entities to make programmatic changes. Implementation plans, unless significant risks need to be mitigated in a timely manner, should allow for Responsible Entities to implement changes on their review cycle or actual events.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Jack Cashin - American Public Power Association - 4	
Answer	No
Document Name	
Comment	
The current implementation plan will require entities to change their CIP-008, as well as EOP-004, reporting. These administrative changes will require system and software changes and planning for the associated resource commitment. Developing the program, gaining consensus internally, training, and testing will take more than 12 months for most entities. APPA recommends a minimum of 18 months for the Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	No
Document Name	
Comment	

Tacoma Power agrees with APPA comments:

"The current implementation plan will require entities to change their CIP-008, as well as EOP-004, reporting. These administrative changes will require system and software changes and planning for the associated resource commitment. Developing the program, gaining consensus internally, training, and testing will take more than 12 months for most entities. APPA recommends a minimum of 18 months for the Implementation Plan."

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

The current implementation plan will require entities to change their CIP-008 as well as EOP-004 reporting. These administrative changes will require system and software changes and planning for the associated resource commitment. Developing the program, gaining consensus internally, training and testing will take more than 12 months for most entities. APPA recommends a minimum of 18 months for the Implementation Plan.

Likes 0	
Dislikes 0	

Response

Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008

Answer	No
Document Name	

Comment

Comments: Given the interest of FERC in expediting the NERC filing, the SPP Standards Review Group believes 6 months is an appropriate timeframe for implementation.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No

Document Name	
Comment	
If not altered, the revised version of CIP-008 is not likely acheivable in 12 months. Or 24 months. It may require additional staff or an outsourced capability that requires longer look-aheads to address budget cycles.	
Likes 0	
Dislikes 0	
Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	
Comment	
With the proposed definition of a Reportable Attempted Cyber Security Incident, a 12-month implementation is not reasonable. The proposed definition will require an increase in staff resources. Given the technical nature involved with tracking and investigating potential “attempts to compromise,” resources are presently limited. Staff would need to be hired and properly trained to implement the processes necessary to meet the requirements. In addition, time is required to research and evaluate tools to be purchased and implemented. A minimal implementation timeframe could result in budgetary constraints or a lack of adequate resources, technology and/or tools.	
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	
Given that these changes will require Responsible Entities to deploy additional resources, modify many existing security processes, potentially implement additional security controls and coordinate these changes across large enterprises, 24 months is a more reasonable timeframe for successful implementation of the necessary changes. ICS-CERT and E-ISAC may also need this time to prepare to receive and act upon this additional reporting.	
Likes 0	
Dislikes 0	
Response	

8. The SDT proposes that the modifications in CIP-008-6 provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable more cost effective approaches, please provide your recommendation and, if appropriate, technical or procedural justification.

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	Yes
Document Name	

Comment

These draft standard changes could require registered entities to install additional monitoring, logging, and alerting systems to be able to acheive the necessary monitoring for adherence to this standard which would be an incremental cost.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	Yes
Document Name	

Comment

No additional comments. .

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	Yes
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS agrees that the proposed revisions provide flexibility, but is concerned that the cost effectiveness and efficiency would be significantly reduced by the continual update requirements proposed within the current draft. As discussed above, there is a potential for the reporting of unverified or uncertain information or the potential taking of action by other utilities in response to non-actionable information. For this reason, AZPS has proposed its comments above, which revisions should align with the SDT's cost-effectiveness and efficiency objectives.	
Likes 0	
Dislikes 0	

Response

Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
This may depend upon the response to question 3.	
Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO, Group Name SPP CIP-008	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Maier - Intermountain REA - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Wagner - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Daniel Frank, Sempra - San Diego Gas and Electric, 3, 5, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Nicole Looney, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Douglas Johnson - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Burns - Stephanie Burns On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Stephanie Burns	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Silvia Mitchell - NextEra Energy - Florida Power and Light Co. - 1,6	
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	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Christopher Overberg - Con Ed - Consolidated Edison Co. of New York - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - CMS Energy - Consumers Energy Company - 1,3,4,5 - RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Quintin Lee - Eversource Energy - 1	
Answer	
Document Name	
Comment	
NC	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
Abstain	
Likes 0	
Dislikes 0	
Response	
Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	

Answer	
Document Name	
Comment	
The proposed changes have the potential to increase work load/overtime costs for those responsible for responding to and reporting attempted incidents.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports the comments provided by NRECA.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Prior to proposing additional modifications, Reclamation recommends each SDT take the necessary time to effectively define the scope of each Standard Authorization Request to minimize the costs associated with the planning and adjustments required to achieve compliance with frequently changing requirements. This will provide entities with economic relief by allowing technical compliance with current standards.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	

Answer	No
Document Name	
Comment	
Any cost determinations can only be evaluated with specific reporting requirements.	
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 Company encourages the SDT to consider modifying the language of M4 to reflect the following:

"Evidence must include, but is not limited to, documentation that collectively demonstrates notification of each determined Reportable Cyber Security Incident according to the applicable requirement parts in *CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents* ***or evidence of active participation in an automated industry information sharing program."***

Southern Company asserts that active participation in an information sharing initiative such as the Cybersecurity Risk Information Sharing Program (CRISP) fully meets the spirit and intent of the reporting requirements outlined in FERC Order 848 and does so in an automated fashion. Technological solutions (like CRISP, DoE CYOTE, etc.) and automation are much better suited for meeting the objectives stated by FERC, where the technology itself is watching for potential incidents and sharing indicators of compromise (IOCs) across the industry in an automated fashion. These programs automatically record Cyber Security Incidents that compromise or attempt to compromise a responsible entity's ESP or associated EACMS. In NERC's publication, *Understanding Your E-ISAC* , they explain[1], "The [CRISP] program enables owners and operators to better protect their networks from sophisticated cyber threats by facilitating the timely sharing of government-enhanced threat information, enhance situational awareness, and better protect critical infrastructure." Putting forth significant additional funding and effort in expanding and maintaining the scope of manual reporting required for CIP-008 will significantly detract from our ability to fully engage in the other worthwhile information sharing projects like CRISP and CYOTE.

Southern Company would also like to reiterate that creating a double reporting burden (the requirement to file the same report to two different agencies) is onerous and ineffective.

[1] Electricity - Information Sharing and Analysis Center, Understanding your E-ISAC, (2016)

Likes 0	
Dislikes 0	
Response	

Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	
Comment	
Identifying and investigating all potential Reportable Attempted Cyber Security Incidents would be time consuming and costly due to the resources required for these tasks. Additional staffing and tools would need to be added. With the present definition, all attempted connections at the EAP/ESP would need to be investigated.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Regular reporting to multiple organizations is not cost effective for a small entity. A more cost effective approach might be a "RC" centric approach, where entities must notify Reliability Coordinators, who are regularly responsible for updating appropriate industry entities.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	No
Document Name	
Comment	
See comments above.	
Likes 0	
Dislikes 0	
Response	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
APPA believes the drafting team has made an effort to meet directives and be flexible, however, the definition for what constitutes a reportable cyber security incident is not distinct, and the proposed reporting requirements are duplicative and will require significant resources to put in place. Consequently the proposal is not cost effective. Suggestions on definition changes and changes to reporting and its implementation are provided in earlier answers.	
Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
Requiring the use of a manual form (Attachment 1) for submitting reports does not provide flexibility and will lead to unnecessary administrative costs for E-ISAC, ICS-CERT and the reporting entities. Including a required form as Attachment 1 in the Standard precludes E-ISAC, ICS-CERT and industry stakeholders from collaborating to develop cost effective and timely reporting methods. In order to replace Attachment 1 with a better reporting tool, the Standard would have to be revised in the future which would add additional ERO and stakeholder expense and time delays. As an alternative, please include Attachment 1 within a guidance document as an option for use in the near term.	
Likes 0	
Dislikes 0	
Response	

Ozan Ferrin - Tacoma Public Utilities (Tacoma, WA) - 5	
Answer	No
Document Name	
Comment	
Tacoma Power agrees with APPA Comments: "APPA believes the drafting team has made an effort to meet directives and be flexible. However, the definition for what constitutes a reportable cyber security incident is not distinct, and the proposed reporting requirements are duplicative and will require significant resources to put in place.	

Consequently, the proposal is not cost effective. Suggestions on definition changes and changes to reporting and its implementation are provided in earlier answers.

Additionally, depending what constitutes an “attempt to compromise or diusrupt,” this may impose a significant forensic burden on enties, depending on how the entity designed its ESP, and Interactive Remote Access solution. For example, if an entity implemented an Interactive Remote Access solution that was accessible to the Internet, they would be exposed to a signigficant number of “attempts to compromise or disrupt.” While this can be done in a secure manner, by design, the attempts could still reach the EACMS system providing remote access to the ESP, and therefore require a significant effort to document and report."

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	No
Document Name	

Comment

APPA believes the drafting team has made an effort to meet directives and be flexible. However, the definition for what constitutes a reportable cyber security incident is not distinct, and the proposed reporting requirements are duplicative and will require significant resources to put in place. Consequently, the proposal is not cost effective. Suggestions on definition changes and changes to reporting and its implementation are provided in earlier answers.

Additionally, depending what constitutes an “attempt to compromise or diusrupt,” this may impose a significant forensic burden on enties, depending on how the entity designed its ESP, and Interactive Remote Access solution. For example, if an entity implemented an Interactive Remote Access solution that was accessible to the Internet, they would be exposed to a signigficant number of “attempts to compromise or disrupt.” While this can be done in a secure manner, by design, the attempts could still reach the EACMS system providing remote access to the ESP, and therefore require a significant effort to document and report.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	No
Document Name	

Comment

Without a clearer definition of attempts, an entity could be overly burdened with administrative and technical tasks associated with investigating, initial reporting and continuous follow-up reporting for insignificant incidents.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

Please see the manor of flexabilty of reporting that has a direct correlation to this.

The use of Attachment 1 should not be mandatory because standards should be objective-based and not technology-dependent. Parts 4.2 and 4.4 - Entities should be allowed to submit reports in any format as long as the report contains the same specified fields of information as described in Attachment 1. We appreciate that the SDT confined the requirements for reporting to the three mandatory items identified in the FERC Order.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	No
Document Name	

Comment

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6

Answer	No
Document Name	

Comment
The proposed changes would take a large number of skilled cybersecurity experts for each RE to investigate and report every attempted Cyber Incident, which adds additional cost without a reduction of risk to the BES. A potential more efficient solution, could be to create an Energy Sector Security Operations Center which aggregates logs from each RE. Creating a Security Opertaions Center, would allow direct reporting to ES-ISAC. It would be more cost effective, provide better metrics with a marco view, allow more flexibility to what FERC wants in the future, and streamline interagency communication processes.

Likes 0	
Dislikes 0	

Response

Brandon McCormick - Brandon McCormick On Behalf of: Carol Chinn, Florida Municipal Power Agency, 6, 4, 3, 5; Chris Gowder, Florida Municipal Power Agency, 6, 4, 3, 5; David Owens, Gainesville Regional Utilities, 3, 1, 5; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 6, 4, 3, 5; Ken Simmons, Gainesville Regional Utilities, 3, 1, 5; Neville Bowen, Ocala Utility Services, 3; Richard Montgomery, Florida Municipal Power Agency, 6, 4, 3, 5; Tom Reedy, Florida Municipal Power Pool, 6; - Brandon McCormick, Group Name FMPA

Answer	No
Document Name	

Comment
FMPA agrees with the following comments submitted by APPA: APPA believes the drafting team has made an effort to meet directives and be flexible. However, the definition for what constitutes a reportable cyber security incident is not distinct, and the proposed reporting requirements are duplicative and will require significant resources to put in place. Consequently, the proposal is not cost effective. Suggestions on definition changes and changes to reporting and its implementation are provided in earlier answers. Additionally, depending what constitutes an “attempt to compromise or diusrupt,” this may impose a significant forensic burden on enties, depending on how the entity designed its ESP, and Interactive Remote Access solution. For example, if an entity implemented an Interactive Remote Access solution that was accessible to the Internet, they would be exposed to a signigficant number of “attempts to compromise or disrupt.” While this can be done in a secure manner, by design, the attempts could still reach the EACMS system providing remote access to the ESP, and therefore require a significant effort to document and report.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment
Entities have no technical basis for the classification of attempted incidents and are left with substantial risk and uncertainty with how to implement the requirements and demonstrate compliance using cost effective approaches. Enforcing the proposed modifications in CIP-008-6 as currently drafted could result in inconsistent implementation resulting in fines and penalties.

Likes 0	
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No
Document Name	

Comment
Identifying and investigating all potential Reportable Attempted Cyber Security Incidents would be time consuming and costly due to the resources required for these tasks. Additional staffing and tools would need to be added. With the present definition, all attempted connections at the EAP/ESP would need to be investigated.

Likes 0	
Dislikes 0	

Response

Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	No
Document Name	

Comment
See comments from the MRO NERC Standards Review Forum.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	

Comment
Utility Services agrees with APPA's comments.

Likes 0	
Dislikes 0	

Response

Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	No
Document Name	

Comment
The additional resources required for data collection, analysis, and reporting could be significant and burdensome, if the proposed criteria for identifying reportable incidents is not revised. Automation seems to be an oversight. The manual process will require hiring additional employees to meet reporting deadlines.

Likes 0	
Dislikes 0	

Response

Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	No
Document Name	

Comment
WAPA agrees that modifications to the standard provide flexibility but WAPA is concerned that there is too much flexibility for interpretation. Auditors and entities will likely **not** agree on the definition of “attempt to compromise.” We suggest further guidance from the SDT. This should be explicitly defined in the requirement and supported with language in the Guidelines and Technical Basis section. We would offer the following examples as a starting point for a more complete list. 1. An “attempt to compromise” could be defined as an act with malicious intent to gain electronic access or to cause harm to the normal operation of a Cyber Asset. a. Actions that are not an attempt to compromise a Cyber Asset electronically include but are not limited to: An entity’s own equipment scanning a Cyber Asset for vulnerabilities or to verify its existence. Broadcast traffic as part of normal network traffic. A firewall may block and log this traffic but it does not have malicious intent.

Attempts to access a Cyber Asset by user that fails due to human error.

b. Actions that are an attempt to compromise a Cyber Asset electronically include but are not limited to:

Scanning a Cyber Asset for vulnerabilities or to verify its existence that is not approved by the entity's management. This could be from an entity's own equipment due to an upstream compromise or malware.

Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given.

2. The word "determination" in Part 4.3 is used relevant to reporting timelines. The standard should require a process to define how this determination is made and by whom. This will allow the entity to clearly define the starting point for the associated timelines.

Likes 0	
Dislikes 0	

Response

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	

Comment

As drafted, the objectives cannot practically be met in a cost effective manner. For example, Tri-State receives around 912,800 attempts per hour on the business network perimeter firewalls. The drafted language could require Tri-State to report on each of those "attempts" which would dramatically increase personnel and record keeping obligations. Additionally, due to the nature of those we would only be able to provide limited information in reporting, which would likely not be enough information for NERC to achieve their objectives.

However, if the modifications proposed in Comments 1 and 4 were incorporated, this would provide Tri-State with flexibility to meet the reliability objectives in a cost effective manner.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro

Answer	No
Document Name	

Comment

Given thate the new definitions would create big amount of unnecessary reportable cyber security incidents, the compliance management cost will be going up largely. See our comments in question 1.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF agrees the changes to the standard provide flexibility but we are concerned that there is too much flexibility for interpretation. Auditors and entities may not agree on the definition of “attempt to compromise.” We suggest additional guidance from the SDT. This could be in the form of the Guidelines and Technical Basis section or a technical rationale document. We would offer the following examples as a starting point for a more complete list.

An “attempt to compromise” could be defined as an act with malicious intent to gain access or to cause harm to the normal operation of a Cyber Asset or a PSP.

Actions that are not an attempt to compromise a Cyber Asset electronically:

An entity’s own equipment scanning a Cyber Asset for vulnerabilities or to verify its existence.

Broadcast traffic as part of normal network traffic. A firewall may block and log this traffic but it does not have malicious intent.

Attempts to access a Cyber Asset by user that fails due to human error.

Actions that are an attempt to compromise a Cyber Asset electronically:

Scanning a Cyber Asset for vulnerabilities or to verify its existence that is not approved by the entity’s management. This could be from an entity’s own equipment due to an upstream compromise or malware.

Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given.

The word “determination” in Part 4.3 is used relevant to reporting timelines. The standard should require a process to define how this determination is made and by whom. This will allow the entity to clearly define the starting point for the associated timelines.

Likes 0	
Dislikes 0	

Response

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6

Answer	No
Document Name	

Comment
Although the proposed modifications provide flexibility, adding EACMS to the applicable assets can be cost intensive as the Responsible Entity will need to additional resources to review events that maybe determined to be Reportable Cyber Security Incidents or Reportable Attempted Cyber Security Incidents

Likes 0	
Dislikes 0	

Response

Adrian Andreoiu - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	

Comment
Given BC Hydro's response and comments to Question #1, BC Hydro does not feel it is appropriate to comment.

Likes 0	
Dislikes 0	

Response

larry brusseau - Corn Belt Power Cooperative - 1	
Answer	No
Document Name	

Comment
I agree the changes to the standard provide flexibility but I am concerned that there is too much flexibility for interpretation. Auditors and entities may not agree on the definition of "attempt to compromise." I suggest additional guidance from the SDT. This could be in the form of the Guidelines and Technical Basis section or a technical rationale document. I would offer the following examples as a starting point for a more complete list. 1. An "attempt to compromise" could be defined as an act with malicious intent to gain access or to cause harm to the normal operation of a Cyber Asset or a PSP. a. Actions that are not an attempt to compromise a Cyber Asset electronically: i. An entity's own equipment scanning a Cyber Asset for vulnerabilities or to verify its existence. ii. Broadcast traffic as part of normal network traffic. A firewall may block and log this traffic but it does not have malicious intent. iii. Attempts to access a Cyber Asset by user that fails due to human error.

b. Actions that are an attempt to compromise a Cyber Asset electronically:

i. Scanning a Cyber Asset for vulnerabilities or to verify its existence that is not approved by the entity's management. This could be from an entity's own equipment due to an upstream compromise or malware.

ii. Attempts to access a Cyber Asset by a user that fails due to not being authorized and intending to gain access where no approval has been given.

2. The word "determination" in Part 4.3 is used relevant to reporting timelines. The standard should require a process to define how this determination is made and by whom. This will allow the entity to clearly define the starting point for the associated timelines.

Likes 0	
Dislikes 0	

Response

Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1

Answer	No
Document Name	

Comment

The manner of reporting needs to be flexible. The use of Attachment 1 should not be mandatory because standards should be objective-based and not technology-dependent. Parts 4.2 and 4.4 - Entities should be allowed to submit reports in any format as long as the report contains the same specified fields of information as described in Attachment 1. We appreciate that the SDT confined the requirements for reporting to the three mandatory items identified in the FERC Order.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Dependent on clarification of the term "attempted" as noted in Question 1, implementation of this Standard could be very cost prohibitive.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP recommends providing additional guidance or define attempt. SRP agrees with the attachment form as an industry template for consistency. If reporting attributes change within 5 days adds administration burden of having the template attachment completed. SRP recommends an adjustment to "when the investigation is complete" so an investigation with all the facts are presented. There is a concern with more reports of Reportable Attempted Cyber Security Incidents may dilute or mask actual real reports.	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The current broad nature of the required reporting could lead to excessive burdens in both reporting as well as analyzing the data. Narrowing the definition of an attempt to only impactful attempts would result in a more cost effective Standard.	
Likes 0	
Dislikes 0	
Response	

9. Provide any additional comments for the SDT to consider, if desired.	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
See comments of the ISO/RTO Council. Also, ERCOT thanks the SDT for their efforts on this revision.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	

Reclamation recommends Requirement R1 Part 1.1 be changed

from:

One or more processes to identify, classify, and respond to Cyber Security Incidents.

to:

One or more processes to identify, classify, handle, and respond to Cyber Security Incidents.

After the change to Requirement R1 Part 1.1 is made, change the measure in Requirement R1 Part 1.1

from:

An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.

to:

An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, handle, and respond to Cyber Security Incidents (e.g., containment, eradication, recovery/incident resolution).

When the change to Requirement R1 Part 1.1 measure is incorporated, remove Requirement R1 Part 1.4.

Reclamation also recommends changing the timeframe specified in Requirement R3 Part 3.2 to 90 days to align with the time allowed in Requirement R3 Part 3.1.

Likes 0	
Dislikes 0	

Response

Todd Bennett - Associated Electric Cooperative, Inc. - 1,3,5,6, Group Name AECI

Answer	
Document Name	

Comment

AECI supports the comments provided by NRECA.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

In Parts 4.3 and 4.4, Dominion Energy recommends clarifying that the determination is the entity's determination for the 5 day clock to begin.

Likes 0	
Dislikes 0	

Response

Jonathan Robbins - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	
Document Name	
Comment	
It is unrealistic to determine the intent of non-human surveillance and reconnaissance as these scans are not actual breach attempts against a network. Port activity analysis using IDS/IPS monitors the potential malicious behavior above and beyond network noise.	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP recommends providing additional guidance or define attempt. Reporting if attributes change within 5 days will add administration burden of having the template attachment completed. SRP recommends an adjustment to when the investigation is complete so a complete investigation with all the facts are presented in the template attachment. There is a concern with more reports of Reportable Attempted Cyber Security Incidents may dilute or mask actual real reports	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	
Document Name	
Comment	
The new/updated standard must address overlap with the existing OE-417.	
Likes 0	
Dislikes 0	
Response	
Anton Vu - Los Angeles Department of Water and Power - 6	

Answer	
Document Name	
Comment	
The new/updated standard must address overlap with the existing OE-417.	
Likes 0	
Dislikes 0	
Response	
Glenn Barry - Los Angeles Department of Water and Power - 5	
Answer	
Document Name	
Comment	
The new/updated Standard must address overlap with the existing OE-417.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
The addition of EACMS functions creates a second definition of the term. If the five functions are what the SDT considers an EACMS to fulfill, the official definition should be modified to include these to avoid differing interpretations of the term based on the Standard.	
Likes 0	
Dislikes 0	
Response	
Terry Harbour - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1	
Answer	
Document Name	

Comment
Change terms to add “Successful” to Reportable “Successful” Cyber Security Incidents in each applicable Requirement/Measure and in CIP-003. Both “Reportable” terms are a mouthful and inevitably will be abbreviated in discussions. This could cause confusion. Adding “Successful” to Reportable Cyber Security Incident would more clearly delineate the difference and could simplify discussions about Cyber Security Incidents being described as Successful or Attempts. For Requirement part 1.2 (and its associated Measure), remove “and requires notification per Requirement R4.” This is redundant with R4. According to the NERC webinar, the SDT’s intent was to remove “notification” from part 1.2 One stop approach – change Requirement 4 to require Registered Entities submit the Attachment 1 content to E-ISAC only. E-ISAC would anonymize it, submit it to ICS-CERT and forward a copy of the submission to the reporting entity as evidence. This preserves confidentiality, simplifies reporting and provides evidence. If Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents must be reported separately to DHS’s ICS-CERT, what does NERC and the SDT propose to do to preserve confidentiality and to protect BES reliability from disclosed infrastructure information when DHS is subject to the Freedom of Information Act? For Requirement part 4.1, remove “Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter,.” This requirement is about defining the content of the report, not defining which scenarios are reportable. If Attachment 1 is mandatory and “unknown” is the only acceptable response when an attribute hasn’t been identified yet, please add an “Unknown” checkbox to make it easier for entities who are dealing with an incident. References to “Click or tap here to enter text.” are out of place because they are not functional and shouldn’t be there. It creates confusion. Attachment 2 Functional Impact examples should reference the reliability tasks referenced in the NERC Functional Model. See footnote 19 on page 13 of the FERC order.

Likes 0	
Dislikes 0	

Response

larry brusseau - Corn Belt Power Cooperative - 1	
Answer	
Document Name	

Comment
The proposed standard has the potential to create a significant auditing burden regarding “attempts to compromise,” which have no impact on reliability. 1. Similar to PRC-004 (normal operations vs. misoperations), there is a much larger population of negatives to prove out versus successful cyber security attempts and incidents to report. PRC-004 audits have required entities to first show definitive documentation to prove a large number of “operations” were classified correctly and were not “misoperations”. If a similar approach is used for this standard, entities will be required to prove the much larger set of negatives before the regulator then audits the positives. 2. Similarly, clarity is needed as to what definitive documentation must be kept for how long for an entity to prove X number of CIP-008-6 “cyber ventures or trials” were not successful CIP-008-6 cyber attempts or incidents.

Finally, the Guidelines and Technical Basis section needs to be updated to reflect the changes to the standard or the technical rationale document needs to be available at the same time the standard is approved. Information in this area assists entities in understanding the intent of the limited wording in the actual requirements. This information also aids entities and auditors when trying to resolve a difference of interpretation. Without this information there is greater risk of an entity not obtaining compliance with the intent of the standard.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

BC Hydro requests explicit clarity on whether Physical Security Perimeter breaches alone without any established breach or compromise of any BES Cyber Systems, ESPs, or EACMS would be considered a potential Reportable Cyber Security Incident. On the NERC led webinar on the CIP-008-6 proposed revisions of October 16, 2018, it was communicated that PSP breaches alone would not constitute a Reportable Cyber Security Incident, however, Requirement 4.1 as written, implies that PSP breaches would constitute potential Reportable Cyber Security Incidents.

Likes 0	
Dislikes 0	

Response

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6

Answer	
Document Name	

Comment

When an event is determined to be a Cyber Security Incident, the Responsible Entitiy needs to determine if it is a Reportable Cyber Security Incident or a Reportable Attempted Cyber Security Incident. The SDT should consider retiring the term Cyber Security Incident. The modified Reportable Cyber Security Incident and the proposed Reportable Attempted Cyber Security Incident definitions provide the identification and required notifications required for the implementation of CIP-008-6.

Likes 0	
Dislikes 0	

Response

Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	

The proposed standard has the potential to create a significant auditing burden regarding “attempts to compromise,” which have no impact on reliability.

1. Similar to PRC-004 (normal operations vs. misoperations), there is a much larger population of negatives to prove out versus successful cyber security attempts and incidents to report. PRC-004 audits have required entities to first show definitive documentation to prove a large number of “operations” were classified correctly and were not “misoperations”. If a similar approach is used for this standard, entities will be required to prove the much larger set of negatives before the regulator then audits the positives.

2. Similarly, clarity is needed as to what definitive documentation must be kept for how long for an entity to prove X number of CIP-008-6 “cyber ventures or trials” were not successful CIP-008-6 cyber attempts or incidents.

Finally, the Guidelines and Technical Basis section needs to be updated to reflect the changes to the standard or the technical rationale document needs to be available at the same time the standard is approved. Information in this area assists entities in understanding the intent of the limited wording in the actual requirements. This information also aids entities and auditors when trying to resolve a difference of interpretation. Without this information there is greater risk of an entity not obtaining compliance with the intent of the standard.

Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	
Document Name	
Comment	

WEC Energy Group is concerned with information protection. The existing information protections that DHS ICS-CERT would use for handling incidents reported to them are unclear. For example, it is unclear whether the reports submitted to DHS will be subject to FOIA requests or whether DHS will make the information reported public. WEC Energy Group recommends clarifying how DHS will handle this information prior to the enforcement date of the proposed Reliabiltiy Standard.

While WEC Energy Group recognizes that any decision regarding the approval of a Reliability Standard must be made on the clear language of the standard, we also believe that having Implementation Guidance as developed by the SDT is an important element to the overall standards development process. For this reason, we ask the SDT to post any Implementation Guidance they have developed with the next ballot.

An additional area where we'd like to see further clarification is related to the definition of Cyber Security Incident. It includes compromise or attempt to compromise (2) Physical Security Perimeter, yet PSPs aren't mentioned anywhere else in the standard except to be explicitly excluded in Requirement R4 part 4.1. We assume the linkage is to CIP-006 Requirement R1.5 and R1.7 which require generation of an alert to Cyber Security Incident Response personnel in the event of detected unauthorized physical access to PSP or PACS. We would like the SDT to spend more time on building and explaining the linkage, especially since CIP-006 only requires alert of an actual breach and the proposed CIP-008 requires notification of breach attempts. Also, rationale for the exception in R4 part 4.1 would be helpful.

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro

Answer	
Document Name	

Comment

1. It is difficult to determine attempts of compromise and SDT should clarify what constitutes an "attempt of compromise". Otherwise, registered entities may have different interpretations resulting in the consistency issue.

2. The timeline statement in Part 4.2 should be moved to Part 4.3 since the Part 4.2 only addresses the notification methods. Also given that the wording "responsible entities "never appears in the Parts, we suggest to remove "responsible entities " from Part 4.2 and reword Part 4.2 as follows:

"One of the following methods for initial notification shall be used:

• Electronic submission of Attachment 1;

• Phone; or

• Email. "

Likes 0	
Dislikes 0	

Response

Ryan Walter - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	
Document Name	

Comment

Regarding Definitions and Reporting: For clarity on current-state reporting and direction for future unforeseen technology and methods, it would be helpful if SDT could provide a list of examples of what would be considered a Reportable Cyber Security Incident versus an Attempt. The list would not

need to be all-inclusive of any potential threats, but would help with consistency and questions. For example, is phishing considered an attempt? The list could be similar in format and methodology to EOP-004 Emergency Preparedness and Operations: Event Reporting.

Regarding R4 and Attachment 1: In order to effectuate recordkeeping, we suggest that after reporting has been submitted, the entity receives a confirmation with a case number. In the event of future updates, the case number can be referenced to locate the records referenced and update the corresponding information. This will also serve as a method to align recordkeeping and maintain evidence that submissions have been received. Alternatively, and at a minimum, the reporting form should include some type of identifier that can be cross-referenced across updates, like a date field (date of the incident, date it was identified, date it was originally reported, etc.)

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5 - WECC, Group Name Seattle City Light Ballot Body

Answer	
Document Name	

Comment

It would be useful if the implementation plan included several examples of instances where the SDT believe are reportable attemps to compromise or disrupt the Electronic Access Control of Monitoring System or the operations of a BES Cyber System. Seattle City Light believes the possible interpretation could be overly broad.

It was discussed on the SDT webinar that “anything out of the normal range of activity” should be considered an attempt. The example being discussed was IP address scanning. One utility might receive random scans 10 times a day on average to a certain address and an other might experience 100 on average. A brighter line defining an attempt and/or examples would be helpful.

Likes 0	
Dislikes 0	

Response

Devin Shines - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	
Document Name	

Comment

We suggest changing the language in “CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents” so that the wording is consistent throughout its contents. Parts 4.2 and 4.4 use the terminology “Responsible Entities shall use…” in the “Requirements” column, whereas Parts 4.1 and 4.3 do not, nor do other standard requirements.

Likes 0	

Dislikes 0	

Response

Debra Boothe - Western Area Power Administration - NA - Not Applicable - WECC	
Answer	
Document Name	

Comment

The proposed standard has the potential to create a significant burden on entities regarding “attempts to compromise,” which have no impact on reliability and will hinder the entities ability to respond to real cyber incidents. The potential increase in investigation and reporting of incidents could lead to a major compromise by allowing bad actors to feint attacks in one area to distract while simultaneously attacking in another area.

WAPA agrees with NSRFs additional comments and includes them with our own.

1. Similar to PRC-004 (normal operations vs. misoperations), there is a much larger population of negatives to prove out versus successful cyber security attempts and incidents to report. PRC-004 audits have required entities to first show definitive documentation to prove a large number of “operations” were classified correctly and were not “misoperations”. If a similar approach is used for this standard, entities will be required to prove the much larger set of negatives before the regulator then audits the positives.

2. Similarly, clarity is needed as to what definitive documentation must be kept for how long for an entity to prove X number of CIP-008-6 “cyber ventures or trials” were not successful CIP-008-6 cyber attempts or incidents.

Finally, the Guidelines and Technical Basis section needs to be updated to reflect the changes to the standard or the technical rationale document needs to be available at the same time the standard is approved. Information in this area assists entities in understanding the intent of the limited wording in the actual requirements. This information also aids entities and auditors when trying to resolve a difference of interpretation. Without this information there is greater risk of an entity not obtaining compliance with the intent of the standard.

ALSO: Reclamation recommends the SDT provide clarifying information to distinguish between the requirements of R1 Part 1.1 and Part 1.4.

Therefore, Reclamation recommends Requirement R1 Part 1.1 be changed

From One or more processes to identify, classify, and respond to Cyber Security Incidents.

to

One or more processes to:

· Identify and classify Cyber Security Incidents.

· Describe handling procedures related to Cyber Security Incidents.

When this change is incorporated, Reclamation also recommends removing requirement 1.4.

Reclamation also recommends specifying that records related to Requirement R2 Part 2.3 be maintained for 15 months following the initial date of reporting the incident to the E-ISAC.

Reclamation also recommends the timeframes specified in Requirement 3 Part 3.2 coincide with the 90 days specified in Requirement R3 Part 3.1, rather than 60 days.

Reclamation also recommends Requirement 4 not include a mandate for entities to notify the ISC-CERT. Replace “ISC-CERT” with the “U.S. Department of Homeland Security” instead of any specific CERT entity within US DHS.	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	
Document Name	
Comment	
Our SMEs believe that responding to an attempted reportable incident should be included as way to test your plan once every 15 months in CIP-008-6 Table R2 2.1.	
Likes 0	
Dislikes 0	
Response	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	
Document Name	
Comment	
Where will reported data be stored? How will the data be protected? Who will be liable for a data breach at E-ISAC or ICS-Cert? Entities will have to spend much time and money to recover from a data breach and to re-secure critical systems.	
Likes 0	
Dislikes 0	
Response	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 3	
Answer	
Document Name	

Comment
While we believe this is a well-thought out modification to CIP-008, we still have concerns regarding the possibility of under or over-reporting as compared to our peers and whether or not being outside of the normal reporting frequency (or bell curve) will create additional scrutiny from regulators. While there is supposed to be a barrier between E-ISAC/ICS-CERT and auditing entities, NERC and the SDT should consider how this separation will be enforced to reduce undue scrutiny for Responsible Entities (REs) who may have varying interpretations of what should and should not be reported. Ensuring clear Implementation Guidance may address this concern. The modification to R1.2 now includes a cross-reference to R4, which adds complexity to interpretation. We recommend this be a separate sub-requirement or otherwise tied in to R4. We noted that the main verbiage in Requirement 4 is structured differently than other CIP requirements which generally instruct REs to implement a plan or process with more specific details included in a sub-part. That information (who to notify) should instead be incorporated into a sub-part for consistency. We are also concerned with information protection. The existing information protections that DHS ICS-CERT would use for handling incidents reported to them are unclear. For example, it is unclear whether the reports submitted to DHS will be subject to FOIA requests or whether DHS will make the information reported public. We recommend clarifying how DHS will handle this information prior to the enforcement date of the proposed Reliability Standard. While we recognize that any decision regarding the approval of a Reliability Standard must be made on the clear language of the standard, we also believe that having Implementation Guidance as developed by the SDT is an important element to the overall standards development process. For this reason, we ask the SDT to post any Implementation Guidance they have developed with the next ballot.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	

Comment
The Guidelines and Technical Basis in CIP-008-6 Draft 1 references a technical rationale document, but this has not been posted. While a technical rationale is not enforceable and cannot change the language of the Standard, it can provide a context within which the understanding of the Standard may change. This document needs to be posted for public review before comments on the revised language of CIP-008-6 Draft 1 will be meaningful. CIP-008-6 R1 Part 1.2 requires the Incident Response Plan to include processes to determine whether an incident is reportable, but does not require a documented process for notification. R4 does not require such a process either. However, the Measures for Part 1.2 reference “documented processes for notification.” If the SDT intends that a process for notification be included in Part 1.2, this should be clearly stated in the Requirement language. CIP-008-6 R4 Part 4.3’s Requirement section contains a parameter, not a Requirement. Suggested wording is, “Responsible Entities shall submit initial notification in accordance with the following timeline: …” The first sentence of the Requirement for CIP-008-6 R4 Part 4.4 requires submission of Attachment 1 updates for new or changed information. The second sentence only requires submissions for new attribute information until all attributes have been reported. The second sentence is contradictory and superfluous to the first sentence and should be deleted.

Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE recommends adding Attempted Reportable Cyber Security Incident to Requirement Parts 3.1 and 3.2 to be consistent with Requirement Part 2.2. If the Cyber Security Incident Response Plan(s) is to be used when responding to an Attempted Reportable Cyber Security Incident (Part 2.2), the plan should also be reviewed and updated after responding (Parts 3.1 and 3.2). With the addition of the definition of Reportable Attempted Cyber Security Incident, Texas RE inquires as to whether that should be included in Requirement Part 2.1. Is a Reportable Attempted Cyber Security Incident considered a test of the entity's plan?	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	
Comment	
NRECA believes it's unrealistic to determine the intent of non-human surveillance and reconnaissance as these scans are not actual breach attempts against a networks. Port activity analysis using IDS/IPS monitors the potential malicious behavior above and beyond general network noise.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	

Comment
Utility Services thinks that the not including "disrupt" in the definition of a Cyber Security Incident in the same way as it is included in the Reportable Cyber Security Incident definition leaves the difference between "compromised" and "disrupted" open to interpretation. We poses that entity definitions for "compromise" and "disrupt" should be included in the same way "programmable" is. In R4, we are concerned with the phrase "or their successors", which could lead to required reporting to all companies or agencies that make a claim to be successors to either E-ISAC or ICS-CERT. If ICS-CERT changes its name, it is still ICS-CERT. If needed, CIP-008 could be revised to reflect the name change in its next update. In M4, Utility Services is concerned that Reportable Attempted Cyber Security Incident is not included, only Reportable Cyber Security Incident. Since R4 includes Reportable Attempted Cyber Security Incident , consistency would be better maintained if M4 included the term as well. On a different note, the word “determined” within M4’s language seems superfluous since R1.2 uses “determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident or Reportable Attempted Cyber Security Incident ”. We think the fact that, in R4.1, the exclusion of Physical Security Perimeter is confusing since the definition of Cyber Security Incident includes Physical Security Perimeter but Reportable Cyber Security Incident does not. By this, a Cyber Security Incident including a compromise to a Physical Security Perimeter **and** Electronic Security Perimeter would not need to be reported since it includes a Physical Security Perimeter. Additionally, in order to maintain consistency with Attachment 1 and R4.2, we propose changing “attributes” to “attribute information”.

Likes 0	
Dislikes 0	

Response

Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	
Document Name	

Comment
We believe it’s unrealistic to determine the intent of non-human surveillance and reconnaissance as these scans are not actual breach attempts against a networks. Port activity analysis using IDS/IPS monitors the potential malicious behavior above and beyond general network noise.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	

Comment

No comment	
Likes 0	
Dislikes 0	
Response	
Scott McGough - Georgia System Operations Corporation - 3	
Answer	
Document Name	
Comment	
GSOC believes it’s unrealistic to determine the intent of non-human surveillance and reconnaissance as these scans are not actual breach attempts against a networks. Port activity analysis using IDS/IPS monitors the potential malicious behavior above and beyond general network noise.	
Likes 0	
Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	
Document Name	
Comment	
See comments from the MRO NERC Standards Review Forum.	
Likes 0	
Dislikes 0	
Response	
William Sanders - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	

E ISAC and ICS-CERT should provide incident reporting / information sharing portals for use by Responsible Entities that meet notification and attribute submittal requirements in the proposed CIP 008-6 modifications.

Likes 0	
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	
Document Name	

Comment

Reporting should be simplified, such as the IP address and service or port that was blocked, and sent periodically (monthly or quarterly) for use by E-ISAC and/or ICS-CERT for correlation across the industry. This simplified reporting would greatly reduce the burden on the entity and still provide the reporting and data necessary to meet the intent of FERC Order No. 848.

Vectren is concerned with information protection. The existing information protections that DHS ICS-CERT would use for handling incidents reported to them are unclear. For example, it is unclear whether the reports submitted to DHS will be subject to FOIA requests or whether DHS will make the information reported public. Vectren recommends clarifying how DHS will handle this information prior to the enforcement date of the proposed Reliabiltiy Standard.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you for allowing Vectren the opportunity to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

CenterPoint Energy understands the objectives of the modifications and their alignment with the FERC directives. However, the concept of “Reportable Attempted Cyber Security Incident” is nebulous. There are past unsuccessful deliberations from attempting to require responsible entities to determine intent as in the efforts to define and enforce “Sabotage Reporting.” The definitions and Requirement 4 have inconsistencies and concepts still to be interpreted. The result of these modifications could be more reporting with little value.

Likes 0	

Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6	
Answer	
Document Name	
Comment	
Attempts to compromise connected systems happen thousands of times every second of every day. They are typically scripted, spoofed, and performed by BOTNETs. BOTNETs can create thousands of attempts per second. Reporting these would be impossible and create significant burden on the RE and NERC. Thank you for allowing us to comment.	
Likes 0	
Dislikes 0	
Response	
Kelsi Rigby - APS - Arizona Public Service Co. - 5	
Answer	
Document Name	Revisions to R4.docx
Comment	
AZPS recommends the change to R4 shown in the attached for clarity.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - 1,3,5 - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI is concerned with information protection. The existing information protections that DHS ICS-CERT would use for handling incidents reported to them are unclear. For example, it is unclear whether the reports submitted to DHS will be subject to FOIA requests or whether DHS will make the	

information reported public. EEI recommends clarifying how DHS will handle this information prior to the enforcement date of the proposed Reliabiltiy Standard.

While EEI recognizes that any decision regarding the approval of a Reliability Standard must be made on the clear language of the standard, we also believe that having Implementation Guidance as developed by the SDT is an important element to the overall standards development process. For this reason, we ask the SDT to post any Implementation Guidance they have developed with the next ballot.

Likes 0	
Dislikes 0	

Response

Douglas Johnson - American Transmission Company, LLC - 1

Answer	
Document Name	

Comment

ATC appreciates the SDT's thoughtful approach to minimize, to the extent possible, modifications to existing language and the mindfulness of unintended consequences. ATC requests that the SDT continue to focus on what, and not how to prevent CIP-008 from becoming overly prescriptive.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	

Comment

Please refer to comments submitted by Edison Electric Institute on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment
Part 1.2 – Remove: '…and requires notification per R4.4' = redundant. You removed the 1 hour requirement in R1.2. Same things on the measures too. *Section 215 INCLUDES PSP – NERC should not start to EXCLUDE it. Recommend striking the following statement from the language: "Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter," out of the language of the requirement. Add a check box in the three fields for attributes, of "unknown" until all attributes have due to the term, "without attributes The 'click or tap…' section is not listed in all three sections, as well as, it is not functional – suggest remove or repair. Change terms to add "Successful" to Reportable "Successful" Cyber Security Incidents in each applicable Requirement/Measure and in CIP-003. Both "Reportable" terms are a mouthful and inevitably will be abbreviated in discussions. This could cause confusion. Adding "Successful" to Reportable Cyber Security Incident would more clearly delineate the difference and could simplify discussions about Cyber Security Incidents being described as Successful or Attempts. For Requirement part 1.2 (and its associated Measure), remove "and requires notification per Requirement R4." This is redundant with R4. According to the NERC webinar, the SDT's intent was to remove "notification" from part 1.2. reporting to the three mandatory items identified in the FERC Order. {C}1. Provide any additional comments for the SDT to consider, if desired. Comments: Part 1.2 – Remove: '…and requires notification per R4.4' = redundant. You removed the 1 hour requirement in R1.2. Same things on the measures too. *Section 215 INCLUDES PSP – NERC should not start to EXCLUDE it. Recommend striking the following statement from the language: "Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter," out of the language of the requirement. Add a check box in the three fields for attributes, of "unknown" until all attributes have due to the term, "without attributes The 'click or tap…' section is not listed in all three sections, as well as, it is not functional – suggest remove or repair. Change terms to add "Successful" to Reportable "Successful" Cyber Security Incidents in each applicable Requirement/Measure and in CIP-003. Both "Reportable" terms are a mouthful and inevitably will be abbreviated in discussions. This could cause confusion. Adding "Successful" to Reportable Cyber Security Incident would more clearly delineate the difference and could simplify discussions about Cyber Security Incidents being described as Successful or Attempts. For Requirement part 1.2 (and its associated Measure), remove "and requires notification per Requirement R4." This is redundant with R4. According to the NERC webinar, the SDT's intent was to remove "notification" from part 1.2 **One stop approach** – change Requirement 4 to require Registered Entities **submit** the Attachment 1 content **to E-ISAC only**. E-ISAC would anonymize it, submit it to ICS-CERT and forward a copy of the submission to the reporting entity as evidence. This preserves confidentiality, simplifies

reporting and provides evidence. If Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents must be reported separately to DHS's ICS-CERT, what does NERC and the SDT propose to do to preserve confidentiality and to protect BES reliability from disclosed infrastructure information when DHS is subject to the Freedom of Information Act?

For Requirement part 4.1, remove "Except for Reportable Cyber Security Incidents compromising or disrupting a Physical Security Perimeter,." This requirement is about defining the content of the report, not defining which scenarios are reportable.

If Attachment 1 is mandatory and "unknown" is the only acceptable response when an attribute hasn't been identified yet, please add an "Unknown" checkbox to make it easier for entities who are dealing with an incident. References to "Click or tap here to enter text." are out of place because they are not functional and shouldn't be there. It creates confusion. Attachment 2 Functional Impact examples should reference the reliability tasks referenced in the NERC Functional Model. See footnote 19 on page 13 of the FERC order.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant Mining Company LLC - 7, Group Name Luminant

Answer	
Document Name	

Comment

We appreciate the hard work of this standard drafting team and the extra burden placed on the team by the accelerated timeline. Our comments are intended to support the team in providing the best solution to this issue with a balance between focusing on a response to the immediate threat, providing timely notification to the appropriate agencies, and addressing the concern of an unwarranted breach of confidential information. - Vistra Energy / Luminant

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 5

Answer	
Document Name	

Comment

E ISAC and ICS-CERT should provide incident reporting / information sharing portals for use by Responsible Entities that meet notification and attribute submittal requirements in the proposed CIP 008-6 modifications.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Allen Klassen, Westar Energy, 6, 3, 1, 5; Bryan Taggart, Westar Energy, 6, 3, 1, 5; Derek Brown, Westar Energy, 6, 3, 1, 5; Grant Wilkerson, Westar Energy, 6, 3, 1, 5; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; James McBee, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; Jennifer Flandermeyer, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; John Carlson, Great Plains Energy - Kansas City Power and Light Co., 5, 1, 3, 6; - Douglas Webb

Answer	
Document Name	

Comment

Single-Point of Data Reporting

The companies are aware of the SDT's discussions and the industry's input regarding: E-ISAC acting as a single point of data acceptance, and E-ISAC forwarding the data to ICS-CERT.

We also have listened to the industry's appeal for an electronic method to submit the required data—an idea that we support. Nevertheless, the companies also recognize there is a limitation of FERC not having regulatory authority to require E-ISAC develop and accept the data through an electronic portal, nor ICS-CERT, for that matter.

With that being the case, and beyond the likely efficiency offered by single-point of data reporting, we have identified a specific concern we believe weakens the proposed CIP-008 revisions; specifically, in the event an electronic, single point of reporting is unavailable to the industry, the proposed CIP-008 revisions will require reallocation of scarce cyber security personnel resources from high-value analysis, monitoring, mitigation, and protection activities to manage inefficient data reporting.

With the potential to weaken security because of reassignment of personnel, we highlight our concern and encourage the SDT to continue its efforts to bring E-ISAC and ICS-CERT into the data submission and reporting methodology discussion.

(Note: "Scarce cyber security personnel resources" refers to the limited pool of available professionals to fill cyber security positions; it is not necessarily a question of expanding cyber security staffs but the competition between all industries to hire trained, experienced, cyber security professionals that can pass background checks.)

Likes 0	
Dislikes 0	

Response

Jack Cashin - American Public Power Association - 4

Answer	
Document Name	

Comment

The information protections that DHS ICS-CERT would use for handling incidents reported to them is not clear and causes concern for APPA. It remains unclear whether the reports submitted to DHS will be subject to Freedom of Information Act (FOIA) requests or whether DHS will consider the

reports public information. APPA believes NERC needs to understand how DHS will classify the data and what confidentiality provisions will be in place, prior to making this an enforceable standard.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	
Document Name	
Comment	
NCPA is in agreement with APPA and USI's comments. Thank you.	
Likes 0	
Dislikes 0	
Response	
Sean Cavote - PSEG - 1,3,5,6 - FRCC,RF, Group Name PSEG REs	
Answer	
Document Name	
Comment	
PSEG supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	

The California ISO supports the comments of the ISO/RTO Council Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	
Document Name	
Comment	
Measure 4 and Requirement R4.1 imply but appear to be missing the insertion of the term “Reportable Attempted Cyber Security Incident”	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	
Document Name	
Comment	
NC	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	
Document Name	
Comment	
The SDT should consider whether adding CIP Exceptional Circumstances to CIP-008 reporting would make sense given some incidents may make reporting difficult for the timelines currently under consideration.	

4.3 High Impact BES Cyber Systems and their associated:

· EACMS

Medium Impact BES Cyber Systems and their associated:

· EACMS

Except when operating under CIP Exceptional Circumstances, theTimeline for initial notification will be:

· One hour from the determination of a Reportable Cyber Security Incident.

· By the end of the next calendar day after a determination of a Reportable Attempted Cyber Security Incident.

Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and ICS-CERT in the form of phone records for preliminary notice or submissions through the E-ISAC and ICS-CERT approved methods, or Attachment 1 submissions.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1, Group Name Exelon Utilities

Answer	
Document Name	

Comment

Like many of our peers, Exelon has concerns regarding the standard not officially defining “attempts”. The drafting team should define parameters where its apparent certain controls have been misused, for example, if authentication credentials were compromised. As well, the drafting team could modify the language to instruct organizations to develop a program or process based on their unqiue characteristics for determining or classifying what the entity classifies an attempt.

Likes 0	
Dislikes 0	

Response

Laurie Williams - PNM Resources - Public Service Company of New Mexico - 1

Answer	
Document Name	

Comment

Agree with the comments made by Lynn Goldstein for PNMR.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	
Document Name	

Comment

Ensure references to "Version 5 CIP Cyber Security Standards" is updated similar to changes made in CIP-002-6.

Recommend the SDT consider adding Physical Security Perimeter or Physical Access Control Systems (PACS) into the applicable systems for CIP-008-6 to ensure any attempts, successful or unsuccessful to compromise the responsible entities PSP or associated PACS are obtained to gain a better understanding of the full scope of cyber-related threats facing the Bulk-Electric Power System(s).

Disagree that Part 4.1 shoulde exclude incidents involving PSPs. The listed items could be applicable to a compromise of a PSP and such incidents should be considered applicable to the entirety of R4.

In Attachment 2 for “Reporting Category” – “Update” field, the reference is to Part 4.2 but appears to be incorrect and should perhaps reference Part 4.4 instead.

As it relates to the SDT not updating the Guidelines & Technical Basis narrative to reflect the changes in CIP-008-6 due to the Technical Ratinale project, it should be considered for removal or updates should be made accordingly. These sections are frequently used by industry and failing to update them could lead to greater confusion.

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	
Document Name	

Comment

Reporting should be simplified, such as the IP address and service or port that was blocked, and sent periodically (monthly or quarterly) for use by E-ISAC and/or ICS-CERT for correlation across the industry. This simplified reporting would greatly reduce the burden on the entity and still provide the reporting and data necessary to meet the intent of FERC Order No. 848.

Vectren is concerned with information protection. The existing information protections that DHS ICS-CERT would use for handling incidents reported to them are unclear. For example, it is unclear whether the reports submitted to DHS will be subject to FOIA requests or whether DHS will make the

information reported public. Vectren recommends clarifying how DHS will handle this information prior to the enforcement date of the proposed Reliabiltiy Standard.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you for allowing Vectren the opportunity to provide comments on this draft standard.

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

In R4, Southern Company is unclear as to the meaning of “United States Responsible Entity.” Does this refer to where an entity is headquartered, or does it refer to the location of the affected cyber systems? Additional clarification regarding the intent of this statement is requested in future revisions of the draft.

Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information. Southern Company is opposed to the SDT addressing the “How” in the Standard. The requirements should dictate “What” information is required to be provided, and to whom, but not “How” entities provide it. Examples of “How” should be deferred to implementation guidance, not imposed as requirements within the Standard.

Likes 0	
Dislikes 0	

Response