Comment Report

Project Name:	2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | CIP-008-6 (Draft 2)
Comment Period Start Date:	11/15/2018
Comment Period End Date:	11/29/2018
Associated Ballots:	2018-02 Modifications to CIP-008 Cyber Security Incident Reporting CIP-008-6 AB 2 ST

There were 72 sets of responses, including comments from approximately 160 different people from approximately 110 companies representing 7 of the Industry Segments as shown in the table on the following pages.

Questions

1. The Standard Drafting Team (SDT) has an updated approach regarding new and modified terms. The SDT is no longer proposing a new definition for reportable attempted cyber security incidents. The defining concepts describing this event have been incorporated in proposed modifications to Requirement R1, Part 1.2.1 and Part 1.2.2. The Responsible Entity will be required to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. The SDT is proposing modifications to Cyber Security Incident as well as Reportable Cyber Security Incident. For Reportable Cyber Security Incident, the SDT has determined it is prudent to include BES Cyber Systems (BCS) because of their criticality in relation to ESPs. By including BCS in the Reportable Cyber Security Incident definition, it shows that Protected Cyber Assets (PCA) are not in scope for the proposed modification. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident? Please provide comments and alternate language, if possible.

2. The SDT has added language in Requirement R1 Part 1.2. for the Responsible Entity to establish and document criteria to evaluate and define attempts in their Cyber Security Incident response plan(s). Do you agree with this approach to allow the entity to define attempts for their unique situation?

3. Do the changes clarify that the Responsible Entity must have a process to determine what is an attempt to compromise and provide notification as stated in Requirement R1 Part 1.2 and Requirement R4 Part 4.2? Please explain and provide comments.

4. 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? Please provide comments and an alternate approach to addressing the directive, if possible.

5. Do you agree with reporting timeframes included Requirement R4 Part 4.2 and Part 4.3 which include an increase in reporting timeframe from 5 to 7 calendar days in Part 4.3? Please explain and provide comments.

6. Do you agree with the SDT's decision to give the responsible entity the flexibility to determine notification methods in their process? Please explain and provide comments.

7. Based on feedback the SDT has adjusted the Implementation Plan timeframe from 12 to 18 months. In the Consideration of Comments Summary Report the SDT justified this change. Do you support the rationale to move to an 18-month Implementation Plan? Please explain and provide comments.

8. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R1 and R4? Please explain and provide comments.

9. 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.

10, 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
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
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
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
Public Utility District No. 1 of Chelan County	Davis Jelusich	6		Public Utility District No. 1 of Chelan County	Joyce Gundry	Public Utility District No. 1 of Chelan County	3	WECC
					Jeff Kimbell	Public Utility District No. 1 of Chelan County	1	WECC
					Meaghan Connell	Public Utility District No. 1 of Chelan County	5	WECC
					Davis Jelusich	Public Utility District No. 1 of Chelan County	6	WECC
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	1,3,4,5,6	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
New York Independent System Operator	Gregory Campoli	2		ISO/RTO Standards Review Committee	Gregory Campoli	NYISO	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Terry BIlke	Midcontinent ISO, Inc.	2	MRO
					Brandon Gleason	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Ali Miremadi	CAISO	2	WECC
					Kahtleen Goodman	ISO-NE	2	NPCC
ACES Power Marketing	Jodirah Green	6	NA - Not Applicable	ACES Standard Collaborations	Eric Jensen	Arizona Electric Power Cooperative, Inc	1	WECC
					Bob Solomon	Hoosier Energy Rural Electric	1	SERC

						Cooperative, Inc.		
					Greg Froehling	Rayburn Country Electric Cooperative, Inc.	3,6	Texas RE
					Chris Bradley	Big Rivers Electric Corporation	1	SERC
					Shari Heino	Brazos Electric Power Cooperative, Inc.	5	Texas RE
					Ryan Strom	Buckeye Power, Inc.	5	RF
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Susan Sosbe	Wabash Valley Power Association	3	RF
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
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
Associated Electric Cooperative, Inc.	Todd Bennett	3		AECI	Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					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) has an updated approach regarding new and modified terms. The SDT is no longer proposing a new definition for reportable attempted cyber security incidents. The defining concepts describing this event have been incorporated in proposed modifications to Requirement R1, Part 1.2.1 and Part 1.2.2. The Responsible Entity will be required to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. The SDT is proposing modifications to Cyber Security Incident as well as Reportable Cyber Security Incident. For Reportable Cyber Security Incident, the SDT has determined it is prudent to include BES Cyber Systems (BCS) because of their criticality in relation to ESPs. By including BCS in the Reportable Cyber Security Incident definition, it shows that Protected Cyber Assets (PCA) are not in scope for the proposed modification. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident? Please provide comments and alternate language, if possible.

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

Answer	Yes
Document Name	

Comment

ERCOT suggests the SDT consider integrating the two definitions together because there is no longer any purpose in distinguishing between a reportable and non-reportable Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

We are in favor of this change, with the note that, while allowing a Responsible Entity to establish the criteria to define the criteria for an “attempt” it leaves the interpretation of the criteria to be scrutinized by an auditor. Historically, auditors have taken issue with a Responsible Entity’s “definition” and caused issues in audits. In this case, because threat vectors and technology constantly change, and new vulnerabilities are discovered every day, it is difficult and problematic to ask Responsible Entities to define an “attempt.” An auditor could easily take issue with a Responsible Entity’s definition or criteria of an attempted compromise.

The proposed VSL is not reasonable because it creates a greater compliance risk without any reducing cyber risk to the BES. Chasing attempts, documenting attempts, and reporting attempts provides no risk reduction to the BES or BCS. Finding attempts only validates the protections within the CIP standards are working properly. Having to report attempts is just burdensome on RE’s.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
While we agree with the proposed modified definition of Reportable Cyber Security Incidnet, AEP recommends that The phrase “that performs one or more reliability tasks of a functional entity” is redundant to the definition of a BCS and should be struck.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA agrees with the proposed modified definitions and with the elimination of ‘reportable attempted cyber security incidents’. BPA appreciates that the SDT recognized entities of varying size face differing threat vectors. BPA supports requiring the Responsible Entity to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems.	
Likes 0	
Dislikes 0	
Response	

Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Concur with EEI comments	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light finds that the revised definitions, focused on BES Cyber Systems, add clarity to the proposed modifications.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Recommend the SDT address/include Physical Security Perimeters in the Reportable Cyber Security Incident definition due to their criticality in relation to BES Cyber Systems and Electronic Security Perimeters.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	

Answer	Yes
Document Name	
Comment	
We agree with the change to include BCS and that PCAs should not be included in the proposed modification to the standard.	
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	
We agree that PCAs should not be in scope.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	Yes
Document Name	
Comment	
Comments: No definition provided for the revised terms.	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	

Answer	Yes
Document Name	
Comment	
Tacoma Power concurs that PCAs should not be included in the proposed modification to the standard.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

While Dominion Energy supports the revised definitions, we suggest a non-substantive change to add clarity and more closely folow the intent of the SDT.

Dominion Energy recommends the SDT consider adding clarity to the definition of Cyber Security Incident that a compromise or attempts to compromise also only applies to the Electronic Security Perimeter and Physical Security Perimeter. This would make it clear that the first bullet only applies to ESP, PSP, and EACMS associated with High and Medium impact BES Cyber Systems. This would relieve our concern the definition can be misinterpreted and would cause a compromise or attempt to compromise an ESP or PSP as defined in the NERC GOT at a low impact facility would be in scope of the definition. Please consider the proposed alternative language:

Cyber Security Incident:

A malicious act or suspicious event that:

- For High or Medium BES Cyber Systems, compromises, or was an attempt to compromise, (1) the Electronic Security Perimeter, (2) the Physical Security Perimeter, or (3) the Electronic Access Control and Monitoring Systems; or
- Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System

Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes

Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren Agrees with and supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
We support the Standards Drafting Team (SDT) modification to Cyber Security Incident and Reportable Cyber Security Incident. Regarding the PCAs as out of scope, Exelon believes it would be beneficial to clarify this out of scope status in the definition of Reportable Cyber Security Incident, which we view as a non-substantive change. Alternatively, Exelon requests clear language in the Implementation Guidance to understand the relationship between the defined terms to avoid confusion and PCAs as out of scope is well documented.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	

EEI appreciates SDT consideration of EEI comments and concerns related to the previously proposed new term, Reportable Attempted Cyber Security Incident and support it's removal. EEI supports the changes made to Requirement R1, parts 1.2.1 and 1.2.2, which address the entity's responsibilities to establish "criteria to evaluate and define attempts to compromise" High and Medium Impact BES Cyber Systems (along with associated EACMS).

We also support the revised definition of "Reportable Cyber Security Incident" as proposed in the current draft.

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	

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

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
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	

Tim Womack - Puget Sound Energy, 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	
Vivian Vo - APS - Arizona Public Service Co. - 3	
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	
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	
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	

Teresa Cantwell - Lower Colorado River Authority - 5	
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	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2	
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	
Julie Severino - FirstEnergy - FirstEnergy Corporation - 1, Group Name FirstEnergy	

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	
Tho Tran - Omaha Public Power District - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
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	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE appreciates the drafting team's efforts to resolve the issues identified in the initial ballot. Texas RE agrees with including BES Cyber Systems in the definitions, however, Texas RE recommends revising the proposed definitions to make it clear which types of Cyber Security Incidents must be reported. FERC Order No. 848 specifically directed NERC "to develop and submit Reliability Standard requirements that require responsible entities to report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS" (paragraph 13). Texas RE suggests that the clearest way to do this is to modify the definition of Reportable Cyber Security Incident, since those are the incidents CIP-008 requires responsible entities to submit. It is confusing to have a definition of Reportable Cyber Security Incident, but it not include everything that is reportable. Texas RE request that the SDT place a priority on having total alignment between all these inter-related aspects for the development of this standard.

Texas RE recommends the following definitions:

- Cyber Security Incident
  - A malicious act or suspicious event that compromises, or was an attempt to compromise or disrupt:
    - the Electronic Security Perimeter(s) or
    - Physical Security Perimeter(s) or,

        - Electronic Access Control or Monitoring Systems, or
        - High or Medium Impact BES Cyber System.
- Reportable Cyber Security Incident
    - A Cyber Security Incident that has compromised or was an attempt to compromise, or disrupted:
        - A BES Cyber System; or
        - Electronic Security Perimeter(s); or
        - Electronic Access Control or Monitoring Systems.

· Texas RE recommends changing "*A BES Cyber System that performs one or more reliability tasks of a functional entity*" to BES Cyber System because the former is redundant. The operation of a BES Cyber System would include performing one or more reliability tasks, per CIP-002-5.1a, Guidelines and Technical Basis, BES reliability operating services starting on pages 16/17 and the definition of a BCA, "*A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adverse ly impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems*."

Additionally, Texas RE noticed the Applicable Systems column does not specifically include ESP(s), which means Part 1.2.2 does not specifically include the scenario for Cyber Security Incidents that attempt to compromise a responsible entity's ESP per FERC Order No. 848. While each ESP should have an associated EACMS, the requirement is not clear that attempts to compromise the ESP is included.

This similarly applied to Part 4.2. The Applicable Systems column does not include ESP(s). This could lead to responsible entities not reporting an attempt to compromise an ESP.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy suggests that "that performs one or more reliability tasks of a functional entity" be removed from the Cyber Security Incident definition. This is already contained in the context of CIP-002 and is superfluous.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	No
Document Name	

Comment

As currently proposed, the Reportable Cyber Security Incident (RCSI) definition does not include compromised BES Cyber Systems (BCS) and individual BCS Cyber Assets (BCA).

Cyber Security Incident (CSI) includes only 2 sets:

1. Compromise (or attempt) of ESP, PSP, EACMS
2. Disruption (or attempt) of BCS (implying BCA)

These sets do not include a compromised BCS or BCA. It only includes BCS/BCA that has been disrupted. Therefore, a definition of RCSI that starts with the CSI definition also does not include a compromised BCS or BCA. Likewise, from R1.2, “an identified CSI [… that is] Only an attempt to compromise…” by definition also does not include include an attempt to compromised a BCS or BCA. However, Figures 2 and 3 in the Implementation Guidance suggest that it is intended that compromised BCS are meant to be reported, at least in the attempted case.

It might be argued that a compromised BCA necessarily means the ESP/EACMS was compromised and so the Incident would be reported anyway, but that is not always true. BCAs can be compromised by communication that is legitimately allowed by an ACL or a firewall rule without that EACMS itself being compromised. A real example would be a filesharing protocol allowed by a firewall being used to compromise a Cyber Asset. TCAs and removable media can do the same, even with the CIP mitigating factors in place.

It is suggested that the CSI definition be clarified to include disruption and compromise for all subpoints the way the RCSI definition does.

A second concern is that the defined term “RCSI” does not in fact include all CSI that are reportable as implied by its name. RCSI should be redefined to include all CSI that are in fact reportable, attempted or otherwise. A new, self-evident name, such as Reportable Cyber Attack (RCA), and a corresponding definition should be adopted for RCSI that are determined to be successful attacks, not just mere attempts. The more stringent reporting requirements would then specifically only apply to those RCA.

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 greatly appreciates the progress that has been made since draft 1 of the standard. Southern asserts that without additional parameters around the specifics of what constitutes an “Attempt to Compromise” the definitions are painted with too broad a brush. Further defining the terms “Cyber Security Incident” and “Reportable Cyber Security Incident” will allow Registered Entities the opportunity to meet the Standard in a clear and measurable way. Additionally, Southern also agrees with the inclusion of the previously proposed “Reportable Attempted Cyber Security Incident” definition so long as the proper scoping is maintained within the words of the definition. See below for alternative wording for the proposed definitions that clarify the meanings and alleviates ambiguity contained within the current proposed definitions.

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

- For high or medium impact BES Cyber Systems, compromised, or was an attempt to compromise, (1) the ESP, (2) the PSP, or (3) the associated EACMS; or
- Disrupted, or was an attempt to disrupt, the operation of a BES Cyber System.

Reportable Attempted Cyber Security Incident – "a *confirmed* malicious act that was determined by the Responsible Entity to be:

- An attempt to compromise the ESP of a high or medium impact BCS; or
- 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 the ESP of a high or medium impact BCS; or
- Disrupted the operation of a BES Cyber System *or high or medium impact-associated EACMS*

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

NRG asserts that the deletion of attachment 1 could cause lack of uniformity of reporting from the industry for meaningful data (i.e. trends in reporting).

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

The proposal to include "attempts to compromise" has the potential to expand the scope of the standard to include corporate assets that are not part of a BCS. This increases the burden to entities for increased monitoring and staffing.

Likes 0	

Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	

Comment
Comments: We agree with the commentary provided by NPCC: • Although there seems to be clarity provided by the NERC drafting team that Protected Cyber Assets were not included in the scope of this project, some entities are confused what the expectation is regarding reporting – specifically is the Entity expected to report on PCAs or not? Some entities have indicated that the NERC webinar and guidance contained some conflicting expectations. • There could be a consistency issue with allowing entities to individually define what is an “attempted” Cyber Security Incident is. Further, the exclusion of PCA’s from required reporting poses a limitation to the industry for gathering and disseminating information on potential or actual threats.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	

Comment
The use of two definitions will be confusing to many. In this version, all Cyber Security Incidents are reportable, as specified by Order 848. The term "Reportable Cyber Security Incident" is unnecessary, as it only identifies a level of reporting for one part (Part 4.2) of CIP-008-6. "Reportable Cyber Security Incident" should be removed and replaced with "Cyber Security Incident."

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	

Comment
Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different. On the proposed definition of Reportable Cyber Security Incident, please clarify that the definition is only associated with the high/medium BES Cyber Systems (BCS).

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	No
Document Name	

Comment
PCA devices pose a weak link in the protection of the ESP and should be considered for incident reporting.

Likes 0	
Dislikes 0	

Response

Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6

Answer	No
Document Name	

Comment
Specificity and clarification on “attempt” is needed for the Responbile Entities to establish appropriate critieria for what is expected to be reported.

Likes 0	
Dislikes 0	

Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	No
Document Name	
Comment	
Specificity and clarification on “attempt” is needed for the Responbile Entities to establish appropriate critieria for what is expected to be reported.	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	No
Document Name	
Comment	
The proposed changes to the CIP standards being proposed by the SDT for 2016-02 (Virtualization) are proposing terminology changes that will directly impact this language as well as how these changes will be interpreted. Further, the “PCA” (or however they will be referred to) should dbe included. This is because by definition they reside inside the ESP and as such if they are compromised or attempted then the rest of the ESP would be at risk.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different.	

On the proposed definition of Reportable Cyber Security Incident, please clarify that the definition is only associated with the high/medium BES Cyber Systems (BCS).	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. Many PCAs perform secondary reliability functions such as GPS timing. Additionally, the Cyber Security Incident Definition speaks to compromise of an ESP. By definition, PCAs are inside an ESP. Based on last Friday's (November 16) NERC's industry webinar (Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting), we understand that PCAs are in the ESP. So Entities are expected to report on PCAs. We request that PCAs be explicitly listed in this table R1's Applicable Systems One could argue that removable media/transient cyber assets could infect a PCA without breaching the ESP. That end result should be reportable since everything in the ESP could be compromised.	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
PCAs should be included in the Applicable Systems column for requirements and in the definitions for Cyber Security Incident and Reportable Cyber Security Incidents due to their association with BES Cyber Systems and potential for revealing malicious activity directed at the BPS.	
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	No
Document Name	
Comment	

PPL NERC Registered Affiliates agree that the new definitions are moving in the right direction, however the current definition changes have created inconsistencies.

For example, a Cyber Security Incident does not take a compromise of a BES Cyber System into account when the new Reportable Cyber Security Incident definition specifically requires entities to report on compromised BES Cyber Systems. Therefore, to improve consistency, we would like to suggest the following addition to the Cyber Security Incident definition.

A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise the, (1) Electronic Security Perimeter, (2) Physical Security Perimeter, or (3) Electronic Access Control or Monitoring Systems for High or Medium Impact BES Cyber Systems, or
- **Compromises or** disrupts, or was an attempt to **compromise or** disrupt, the operation of a BES Cyber System

Even though Order 848, paragraph 3, does not directly state in the reporting directive that BES Cyber Systems should be included as part of the “Cyber Security Incidents that compromise, or attempt to compromise”, paragraph 19 of the discussion points out that “*unsuccessful attempts to compromise* or disrupt a responsible entity’s core activities are not subject to the current reporting requirements in Reliability Standard CIP-008-5 or elsewhere in the CIP Reliability Standards” (emphasis added). Therefore, we agree with the SDT that it is prudent to include BES Cyber Systems in the definition of Reportable Cyber Security Incident.

We do not agree, however, with the scope of the edits to the definition. We believe that by including BES Cyber System and removing “that perform one or more reliability tasks of a functional entity”, it will accomplish what the SDT has stated was their goal. Therefore, we suggest the following edits to the Reportable Cyber Security Incident definition:

"A Cyber Security Incident that has compromised or disrupted:

A BES Cyber System;

Electronic Security Perimeter(s); or

Electronic Access Control or Monitoring Systems."

Likes 1	ISO New England, Inc., 2, Puscas Michael
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	

We agree with SDT's decision to NOT create a new proposed term for Reportable Attempted Cyber Security Incident. Thank you for this change from the first posting.

We agree with this posting's proposed modifications to Cyber Security Incident. The proposed changes, though more detailed, respect the content the definition of cyber security incident in Section 215 of the Energy Policy Act of 2005.

We disagree with the proposed modifications to Reportable Cyber Security Incident for two reasons.

First. We accept the addition of "A BES Cyber System" in the first bullet. However, we recommend deleting the rest of the bullet as redundant and adding confusion. Delete "that performs one or more reliability tasks of a functional entity." This is unnecessary because it is redundant to content in the NERC Glossary definition of BES Cyber System."

Second. FERC Order 848 directed "NERC to develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)." It will be clearer to address the directive in the definition of Reportable Cyber Security Incident. We recommend: "A Cyber Security Incident that: compromised or disrupted a BES Cyber System; or compromised or attempted to compromise an Electronic Security Perimeter; or compromised or attempted to compromise Electronic Access Control or Monitoring Systems." This uses language from the FERC Order and is clearer than this proposed posting.

Likes 1	ISO New England, Inc., 2, Puscas Michael
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST recommends that the SDT ELIMINATE the definition of "Reportable Cyber Security Incident." FERC has directed that ALL security events determined to be "Cyber Security Incidents" be reported, which renders the definition of "Reportable Cyber Security Incident" needlessly redundant (and confusing to the casual reader). N&ST believes the different reporting deadlines for attempted vs. actual compromises and/or disruptions can be adequately addressed in Requirement R4. N&ST notes that adopting this recommendation would necessitate minor changes (to eliminate "Reportable Cyber Security Incident") to Requirements R1 through R4. Finally, N&ST strongly recommends that Protected Cyber Assets (PCAs) be considered "Applicable Systems" and included in both the definition of "Cyber Security Incident" and the CIP-008 requirements.

Likes 0	
Dislikes 0	

Response
Brian Evans-Mongeon - Utility Services, Inc. - 4
Answer	No
Document Name	
Comment
We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. The Cyber Security Incident Definition speaks to compromise of an ESP but does not include PCAs. Since, by definition, PCAs are inside an ESP, it could be determined that Entities are expected to report on PCAs. We request that the ambiguity be cleared up by explicitly listing PCAs in table R1's Applicable Systems.
Likes 0	
Dislikes 0	
Response
larry brusseau - Corn Belt Power Cooperative - 1
Answer	No
Document Name	
Comment
Please note that even thought I agree with the flexibility to establish my own criteria, I believe that this flexibility will be addressed in a future NOPR as all applicable Entities will have different criteria of what an attempt to compromise is.
Likes 0	
Dislikes 0	
Response
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5
Answer	No
Document Name	
Comment
NV Energy agrees with the SDT's decision to not create a new proposed term for Reportable Attempted Cyber Security Incident. We appreciate the SDT listening to industry comment on this.

NV Energy agrees with this posting's proposed modifications to Cyber Security Incident. The proposed changes, though more detailed, respect the content the definition of cyber security incident in Section 215 of the Energy Policy Act of 2005.

NV Energy would respectively disagree with the proposed modifications to Reportable Cyber Security Incident for two reasons.

- We accept the addition of "A BES Cyber System" in the first bullet. However, we recommend deleting the rest of the bullet as redundant and adding confusion. Delete "that performs one or more reliability tasks of a functional entity." This is unnecessary because it is redundant to content in the NERC Glossary definition of BES Cyber System."

- FERC Order 848 directed "NERC to develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)." It will be clearer to address the directive in the definition of Reportable Cyber Security Incident. We recommend: "A Cyber Security Incident that: compromised or disrupted a BES Cyber System; or compromised or attempted to compromise an Electronic Security Perimeter; or compromised or attempted to compromise Electronic Access Control or Monitoring Systems." This uses language from the FERC Order and is clearer than this proposed posting.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

We disagree with the proposed modifications to Reportable Cyber Security Incident for two reasons:

First. We accept the addition of "A BES Cyber System" in the first bullet. However, we recommend deleting the rest of the bullet as redundant and adding confusion. Delete "that performs one or more reliability tasks of a functional entity." This is unnecessary because it is redundant to content in the NERC Glossary definition of BES Cyber System."

{C}1. definition, it shows that Protected Cyber Assets (PCA) are not in scope for the proposed modification. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident? Please provide comments and alternate language, if possible.

Yes

No

Comments: We disagree with the proposed modifications to Reportable Cyber Security Incident for two reasons:

First. We accept the addition of "A BES Cyber System" in the first bullet. However, we recommend deleting the rest of the bullet as redundant and adding confusion. Delete "that performs one or more reliability tasks of a functional entity." This is unnecessary because it is redundant to content in the NERC Glossary definition of BES Cyber System."

Second. FERC Order 848 directed, "NERC to develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access

Control or Monitoring Systems (EACMS).” It will be clearer to address the directive in the definition of Reportable Cyber Security Incident. We recommend: “A Cyber Security Incident that: compromised or disrupted a BES Cyber System; or compromised or attempted to compromise an Electronic Security Perimeter; or compromised or attempted to compromise Electronic Access Control or Monitoring Systems.” This uses language directly from the FERC Order and is clearer than this proposed posting without using excess uneccessary language.

We agree with this posting’s proposed modifications to Cyber Security Incident. The proposed changes, though more detailed, respect the content the definition of cyber security incident in Section 215 of the Energy Policy Act of 2005.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. Many PCAs perform secondary reliability functions such as GPS timing. Additionally, the Cyber Security Incident Definition speaks to compromise of an ESP. By definition, PCAs are inside an ESP.

Based on last Friday’s (November 16) NERC’s industry webinar (Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting), we understand that PCAs are in the ESP. So Entities are expected to report on PCAs. We request that PCAs be explicitly listed in this table R1’s Applicable Systems

One could argue that removable media/transient cyber assets could infect a PCA without breaching the ESP. That end result should be reportable since everything in the ESP could be compromised.

Otherwise we agree

Likes 0	
Dislikes 0	

Response

Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle

Answer	No
Document Name	

Comment

We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. Many PCAs perform secondary reliability functions such as GPS timing. Additionally, the Cyber Security Incident Definition speaks to compromise of an ESP. By definition, PCAs are inside an ESP.

Based on last Friday's (November 16) NERC's industry webinar (Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting), we understand that PCAs are in the ESP. So Entities are expected to report on PCAs. We request that PCAs be explicitly listed in this table R1's Applicable Systems

One could argue that removable media/transient cyber assets could infect a PCA without breaching the ESP. That end result should be reportable since everything in the ESP could be compromised.

Otherwise we agree

Likes 0	
Dislikes 0	

Response

2. The SDT has added language in Requirement R1 Part 1.2. for the Responsible Entity to establish and document criteria to evaluate and define attempts in their Cyber Security Incident response plan(s). Do you agree with this approach to allow the entity to define attempts for their unique situation?

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

Answer	Yes
Document Name	

Comment

NRG does not have concerns about the Responsible Entities ability to evaluate and define “attempts at compromise” however; NRG asserts that the lack of uniformity in the reporting (i.e. deletion of Attachment 1) could cause difficulty in assessment of the data by E-ISAC and NCCIC, and the resulting conclusions may not be useful to the industry.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	Yes
Document Name	

Comment

This additional language to R1 Part 1.2 leaves a Responsible Entity’s criteria and definition open to interpretation by an auditor which is concerning.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

CenterPoint Energy Houston Electric, LLC (CenterPoint Energy or Company) agrees with this approach, but would like to note that many events are not attempts or reportable. The Company also requests that the Standard Drafting Team be conscious of including systems that are out of scope as BES Cyber Systems or Electronic Access Control and Monitoring Systems in the Implementation Guidance.

Likes 0	

Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	

Comment
While responsible entities should be encouraged to address this definition of “attempt to compromise or disrupt” related to a Cyber Security Incident, some care should be taken to ensure a minimum level of diligence is expressed in such a definition. A simple form of definition might include documenting judgement of a cyber security analyst at a particular time as the means to determine an attempt (“I’ll know one when I see it”). This may pose some difficulty for auditors trying to assess compliance to this part of the standard. Note: *ERCOT is excluded from the group for this response.*

Likes 0	
Dislikes 0	

Response

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
EEI supports the revised language in Requirement R1, Part 1.2; which we believe appropriately places the responsibility for establishing and documenting criteria to evaluate and define attempts to compromise “identified” systems within the responsible entity’s Cyber Security Incident response plan(s). We believe this change will provide entities with the flexibility to tailor criteria in ways that align with their internal processes and procedures to provide clarity and effective reporting.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	

Comment

We agree this update allows RE's the ability to establish a solid program.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. The Cyber Security Incident Definition speaks to compromise of an ESP but does not include PCAs. Since, by definition, PCAs are inside an ESP, it could be determined that Entities are expected to report on PCAs. We request that the ambiguity be cleared up by explicitly listing PCAs in table R1's Applicable Systems.	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren Agrees with and supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes

Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
In addition, PCAs should be included in the Applicable Systems column for requirements and in the definitions for Cyber Security Incident and Reportable Cyber Security Incidents due to their association with BES Cyber Systems and potential for revealing malicious activity directed at the BPS.	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	Yes
Document Name	
Comment	
Tacoma Power supports the intent of the proposed changes. However, we also recognize that Standard still needs and would benefit from guidance on alternative approaches addressing the language,“*establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems.”* We are concerned that without established guidance, complying entities and compliance and enforcement staff do not have sufficient guidance to come to common understanding of the draft standard language. Complying public power entities believe that a conservative reporting criteria will present significant costs to administer, without corresponding measurable reliability benefits. The costs required for the follow-up requirements in R4 are significant.	
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	
SDT should consider a minimum criteria for the definition of an “attempt”.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light appreciates the efforts of the SDT to provide guidance about how an entity might evaluate and define attempts, and finds that guidance sufficient in general.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Concur with EEI comments	
Likes 0	

Dislikes 0	
Response	
Andy Fuhrman - Andy Fuhrman On Behalf of: Theresa Allard, Minnkota Power Cooperative Inc., 1; - Andy Fuhrman	
Answer	Yes
Document Name	
Comment	
These changes are effective when considering how a particular entity can maintain compliance with this standard. Unfortunately, the lack of a universal definition of "attempt" will result in poor data that fails to provide a complete picture of the threat landscape based on attempts across the ERO. A quality standard that addresses both the compliance needs of the industry and the information/data needs of the ERO could have been drafted had the drafting team been given more time and a more thoughtful FERC order.	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	Comments for Question 2.docx
Comment	
Please see the attachment for AZPS's response.	
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	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
While responsible entities should be encouraged to address this definition of “attempt to compromise or disrupt” related to a Cyber Security Incident, some care should be taken to ensure a minimum level of diligence is expressed in such a definition. A simple form of definition might include documenting judgement of a cyber security analyst at a particular time as the means to determine an attempt (“I’ll know one when I see it”). This may pose some difficulty for auditors trying to assess compliance to this part of the standard.	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by NRECA	
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	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
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	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Omaha Public Power District - 1 - Texas RE	
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	
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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
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	
Eric Smith - NaturEner USA, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tommy Drea - Dairyland Power Cooperative - 5	
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	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
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	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
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	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
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	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE is concerned that allowing Responsible Entities to establish its own criteria to evaluate and define attempts to compromise (Subpart 1.2.1) will lead to inconsistencies in what is reported which may limit the value of the reported data. Texas RE requests the SDT to define a criteria or reporting threshold for the Cyber Security incidents described in the FERC order. Please see Texas RE's comments in #1 regarding the change to the definition of Reportable Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	No

Document Name	

Comment

What constitutes an “attempt” should be clearly defined in the standard so that a uniform reporting obligation applies industry-wide. If the purpose of the reporting mandate is to ensure reporting of accurate risk information to E-ISAC and NCCIC for their own analytical purposes and for the purpose of sharing credible threat information with industry, the reporting of that information should be standardized and not left to the judgment of each responsible entity. Furthermore, without a standard definition, responsible entities may be vulnerable to an enforcement determination that the entity’s definition of “attempts” is inadequate. A clear definition helps entities ensure that they are complying with the rule. While the proposed Implementation Guidance is helpful in some respects, it is not obligatory, and therefore leaves open the possibility of a multiplicity of reporting practices. The SDT should consider adopting a list of indicators such as those suggested by the ISO/RTO Council in its comments to FERC in the rulemaking in Docket No. RM18-2.

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 has a few concerns with R1, primarily R1.2.1 where the entity must have “One or more processes to establish criteria to evaluate and define attempts to compromise.” We don’t think FERC’s intent for the requirement really is for entities to have a “process to establish criteria.” Entities can establish criteria or have a process to determine whether an event is a true, confirmed attempt to compromise and is reportable, but we don’t think a process to determine the criteria meets the intent of the FERC Order. There is also concern over determining what the possible criteria would be for an attempted compromise. In the absence of a defined term, an attempt that rises to the level of reportability remains very subjective. It would include events that are confirmed as having a malicious intent but aren’t script kiddies or just the normal innocuous noise. It’s not every dropped packet at a firewall but could be some. It’s not every phishing email but could be some. It’s not every failed remote SSH login but could be some. The threshold is going to depend on the facts and circumstances of each event and defies being able to sit down and put into objective and measurable criteria ahead of time. This is why the definitions we have proposed both properly scope reportable incidents as either attempts or actual compromises, and provides the Responsible Entity the levity to make those determinations.

Southern suggests that “establish criteria” be dropped since this problem defies reducing to simple criteria and be replaced by a “process to determine which Cyber Security Incidents should be reported as attempts to compromise.”

Requirement R1.2:

One or more processes to:

1.2.1 Determine if an identified Cyber Security Incident is:

- A Reportable Attempted Cyber Security Incident; or

- A Reportable Cyber Security Incident; and

1.2.2 Provide notification per Requirement R4.

Note: One or more processes to identify, classify, and response to a Cyber Security Incident is already defined as per R1.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy agrees that it is correct for Responsible Entities (RE) to define attempts for their unique programs; however, we are concerned with the language of Requirement R1 1.2. Xcel Energy respectfully suggests removing R1.2.1 in its entirety. R1.1 requires REs to identify Cyber Security Incidents and R1.2.2 requires REs to determine if a Cyber Security Incident is a Reportable Cyber Security Incident or an attempt to compromise. Having an additional enforceable Requirement to establish a set of criteria or methods to evaluate is not needed and is not in the spirit of the Efficiency review project currently under way.

If the Standard Drafting Team choses to go ahead with the language in R1.2.1, Xcel Energy would then suggest that the term “criteria” be removed from the Requirement language. We believe the term "Criteria," is too prescriptive when trying to establish what would be considered an attempt and that a cyber security event that should be reported may not fit into a REs pre-defined set of criterion. We believe that the R1.2.1 should be reworded to read: Have one or more process to: "Establish a documented evaluation method that may include using criteria or other evaluation processes to define attempts to compromise.” This would allow for methods other than a set of prescriptive criteria to evaluate non-conventional events that may not meet established criterion to also be considered as an attempt to compromise but could through some other form of methodology or assessment ultimately be deemed an attempt to compromise. This allows the Requirement language to be flexible enough to ensure entities are able to modify their programs as needed to effectively meet future risks in a changing environment.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	No
Document Name	

Comment

: We disagree with the changes made to Requirement R1, part 1.2.1, which addresses the entity's responsibilities to, "Establish criteria to evaluate **and define** attempts to compromise;"

Recommend remove the term "define," and keep the established scope per NERC, CIP & FERC as: ...

The language would have to be so ubiquitous to cover changes in technologies and encapsulate outlying behavior, that any documented process would be outmoded – and in CONSTANT revisions.

R1.1. already has a criteria to identify the attempts. R.1.1 - One or more processes to identify, classify, and respond to Cyber Security Incidents.)

No - For part 1.2.1, removing "define" allows the entity more flexibility to scope attempts to compromise into their criteria for evaluating the Cyber Security Incident.

R1.2 - One or more processes to: Use: "Respond"?

1.2.1 Establish criteria to evaluate and define attempts to compromise;

1.2.2 Determine if an identified Cyber Security Incident is:

{C}· A Reportable Cyber Security Incident or

{C}· Only an attempt to compromise one or more systems identified in the "Applicable Systems" column identified for this Part;

1.2.3 Provide notification per as specified in Requirement R4 of this Standard.

"**Attempts**" have been a part of the definition for a Cyber Security Incident for more than a decade. PAC will not support a process to define "attempts." Industry has already been identifying attempts for years. Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity's existing program(s). Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain. Per our comments on question 1, we recommend incorporating the FERC directive for "attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)" in the Reportable Cyber Security Incident definition. Part 1.2 would retain "One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident." The rest of existing Part 1.2 would be deleted.

Further, we disagree with the proposed Part 1.2 to include any reference to "provide notification per Requirement R4." This recreates a cross-reference between two requirements and potential double jeopardy for noncompliance. Part 1.2 should have NO reference to reporting.

Additionally, **we disagree with the proposed language changes in the Requirements column for Parts 2.2. and 2.3** With our proposed changes from question 1 and this question, Parts 2.2 and 2.3 should only be modified in the Applicable Systems column. There is no question in the comment form for Part 2.2 or 2.3

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment

“Attempts” have been a part of the definition for a Cyber Security Incident for more than a decade. NV Energy does not support a process to define “attempts.”

Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity’s existing program(s). Every additional change in the terms or Parts creates additional work for Entity’s to revise, implement and retrain. Per our comments on question 1, we recommend incorporating the FERC directive for “attempt to compromise, a responsible entity’s Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)” in the Reportable Cyber Security Incident definition. Part 1.2 would retain “One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident.” The rest of existing Part 1.2 would be deleted.

Further, we disagree with the proposed Part 1.2 to include any reference to “provide notification per Requirement R4.” This recreates a cross-reference between two requirements and potential double jeopardy for noncompliance. Part 1.2 should have not have a reference to reporting.

Likes 0	
Dislikes 0	

Response

larry brusseau - Corn Belt Power Cooperative - 1

Answer	No
Document Name	

Comment

Please note that even thought I agree with the flexibility to establish my own criteria, I believe that this flexibility will be addressed in a future NOPR as all applicable Entities will have different criteria of what an attempt to compromise is.

Likes 0	
Dislikes 0	

Response

Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County

Answer	No
Document Name	

Comment

While the flexibility for entities to define "attempts to compromise” in their unique situations may be desirable, guidance should be provided outlining the characteristics common to these attempts.

Likes 0	

Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment
If the SDT deems it important to add an explicit requirement to define and document criteria for identifying Cyber Security Incidents (it's already implied by the language of existing CIP-008 R1 Part 1.1), N&ST believes it should be added to R1 Part 1.1, not R1 Part 1.2. N&ST also recommends changes to the proposed of language of R1 Part 1.2.2. Per FERC's directive, all Cyber Security Incidents are to be considered "reportable" (N&ST also recommends eliminating the definition of "Reportable Cyber Security Incident," as per our response to Question 1). N&ST agrees that an actual compromise of an ESP or an applicable system should be distinguished from an (unsuccessful) attempt but objects to the use of the word, "only" (as in "Only an attempt..."), as it implies triviality. Suggested re-wording: "Determine whether an identified Cyber Security Incident was an attempt to compromise an ESP or an applicable system or actually compromised or disrupted an ESP or an applicable system."

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
"Attempts" have been a part of the definition for a Cyber Security Incident for more than a decade. MEC will not support a process to define "attempts." Industry has already been identifying attempts for years. Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity's existing program(s). Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain. Per our comments on question 1, we recommend incorporating the FERC directive for "attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)" in the Reportable Cyber Security Incident definition. Part 1.2 would retain "One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident." The rest of existing Part 1.2 would be deleted. Further, we disagree with the proposed Part 1.2 to include any reference to "provide notification per Requirement R4." This recreates a cross-reference between two requirements and potential double jeopardy for noncompliance. Part 1.2 should have NO reference to reporting. Additionally, we disagree with the proposed language changes in the Requirements column for Parts 2.2. and 2.3 With our proposed changes from question 1 and this question, Parts 2.2 and 2.3 should only be modified in the Applicable Systems column. There is no question in the comment form for Part 2.2 or 2.3

Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	No
Document Name	
Comment	
LES has ongoing concerns about the lack of a clear and concise definition for “attempt to compromise”, but does understand the challenge of creating a one size fits all definition. The guidance document developed by the drafting team provides good examples of what does and what does not constitute an attempt to compromise.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
The lack of any guidance for industry to review makes it very difficult for us to provide a more productive set of comments. It would be very helpful if additional specifics on what would justify as an “attempt to compromise” were provided in guidance, which would reduce confusion during a regulatory engagement.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	

Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

Comments: Further clarification on what qualifies as an attempt to compromise a system, and a definition of “attempt” are needed.

Likes 0	
Dislikes 0	

Response

Seth Shoemaker - Muscatine Power and Water - 3

Answer	No
Document Name	

Comment

While having the flexibilty to establish and document our own criteria may be beneficial, we believe this leaves too much room for interpretation and may not address the security objectives of the Standard if an entity chooses not to include specific criteria in their plans. Additionally, because entities will establish and document independent criteria, this creates room for auditors to determine their preferred criteria and attempt to hold entities to that Standard. We recommend the SDT establish and document minimum required criteria to evaluate and define attempts to compromise to create a baseline for entities to be held to.

Likes 0	
Dislikes 0	

Response

Michael Buyce - City Utilities of Springfield, Missouri - 1

Answer	No
Document Name	

Comment
While it is makes sense that each Responsible Entity will be required to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems, there is some concern on the auditablility of such a requirement. There is concern that without a more clear objective in the requirement, a Responsible Entity may have implemented, in good faith, a criteria to evaluate and define an attempt to compromise; however, an auditor may not agree, thus resulting in a potential instance of noncompliance.

Likes 0	
Dislikes 0	

Response

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

Comment
One of the four elements outlined by FERC was to improve the quality of reporting and allow for ease of comparison. In order to collect consistent data across all Responsible Entities it is necessary to provide specificity to “attempt”.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	

Comment
Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No

Document Name	

Comment

Part 1.2 is unnecessary and duplicative of Part 1.1. The language of Part 1.2.1 and Part 1.2.2 describes some parts of the classification of a Cyber Security Incident, which is required by Part 1.1. Part 1.2.3 specifies notification, which is part of response required by Part 1.1. Any language needed to clarify the basic requirements of "identify, classify, and respond" should be included in Part 1.1, not a separate Part.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

: If the satandard as written is approved, then Responsible Entities should be allowed to define attempts based on their environment configuration, however, the proposal to include "attempts to compromise" has the potential to expand the scope of the standard to include corporate assets that are not part of a BCS. This increases the burden to entities for increased documentation of attempts.

Likes 0	
Dislikes 0	

Response

Leanna Lamatrice - AEP - 3

Answer	No
Document Name	

Comment

AEP believes if all the RE’s have their own criteria to evaluate and define then Responsible Entities run the risk of reporting (or not reporting) different incidents. While it is challenging to come up with a common definition of a reportable incident, consistency is needed to ensure the appropriate CSI’s are reported to satisfy FERC Order 848.

Likes 0	
Dislikes 0	

Response

3. Do the changes clarify that the Responsible Entity must have a process to determine what is an attempt to compromise and provide notification as stated in Requirement R1 Part 1.2 and Requirement R4 Part 4.2? Please explain and provide comments.

Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

In R1.2.2 the term “only” is introduced in the Requirement language, in the Measures, and is also used in the Requirement language of R4.2. Xcel Energy believes that the use of the term “only” may create a situation in which a Responsible Entity (RE) would need to prove to an auditor that an event was in fact “only” an attempted event and not an actual compromise. This would put a RE in a position where they would need to prove the negative. By removing “only” from the Standard language it will remove the implication that a RE has made that permanent determination that it was an attempt. The removal of “only” will not substantively change the intent of the Requirement. We see this as an important change to ensure that attempts to compromise are promptly reported while still allowing on-going monitoring and evaluations to determine if an actual compromise has occurred which in some cases could be some time in the future.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

AECI supports comments provided by NRECA

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	
Please note that even though the NSRF agrees with our flexibility to establish our own criteria, we believe that this flexibility will be addressed in a future NOPR as all applicable Entities will have different criterias of what an attempt to compromise is.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Concur with EEI comments	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light finds the changes clarifying, and finds the additional guidance helpful in developing an acceptable process to determine what is an attempt to compromise.	
Likes 0	

Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
An entity's processes for Part 1.2 should include establishing criteria to evaluate incidents (Part 1.2.1), determine if Cyber Security Incidents are Reportable or an attempt (Part 1.2.2), and how to provide R4 notifications including each Part of R4 (Part 1.2.3). Thus, the entity's Part 1.2 process(es) must address *what* is included in initial notifications (Part 4.1), when they are to be submitted after determinations (Part 4.2), and how to provide updates as determined with new or changed attribute information within 7 days (Part 4.3). Consequently, the entity's determination utilizing the Part 1.2 process should lead to initial notifications outlined in Part 4.2.	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Referring to the “Applicable Systems” column in the “Requirements” column may be redundant. A suggestion for the language in the second bullet for Part 1.2.2 is: “An attempt to compromise (as defined in Part 1.2.1) one or more applicable systems.”	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
However, guidance from the SDT would be appreciated to set a baseline for what an attempt to compromise is to ensure consistent application of the requirements.	

Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	Yes
Document Name	
Comment	
Tacoma Power believes that the proposed changes reflect that an Entity must have a process in place identify compromise attempts and provide notification. Tacoma Power is concerned that specifying a specific number of days for reporting actual and attempted Cyber Security Incidents to agencies will sometimes be a resource challenge. Tacoma Power recommends that the SDT consider a time frame that provides an update within 24 hours of actual determination of the criteria established in R4.1. Physically getting a team to remote substations to determine the attack vector could take time and difficulty will be increased depending the how wide-spread the event turns out to be.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren Agrees with and supports EEI Comments	

Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We recommend that High and Medium BES Cyber System associated PCAs should be included in the Applicable Systems column for Requirement 1 because PCAs could be a vector for compromise. Additionally, the Cyber Security Incident Definition speaks to compromise of an ESP. By definition, PCAs are inside an ESP.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI believes the proposed language clearly defines that responsible entities must have processes in place within their Cyber Security Incident Response plans that determine what an attempt to compromise is along with their reporting responsibilities. Although we support the revised language in Requirement R1 Part 1.2 and Requirement R4 Part 4.2, we suggest the SDT consider making the following minor modification to the phrase “only an attempt to compromise” to “an attempt to compromise”. (see Subpart 1.2.2, Measures for Part 1.2, Measures 2.3 and Requirement R4) Although we understand the SDT’s reasoning for adding “only” to the phrase, we believe it offers little additional clarity yet does have the potential for adding confusion to the phrase. Moreover, within Requirement 1, Subpart 1.2.1 entities are clearly required to define “attempts to compromise”.	
Likes 0	
Dislikes 0	
Response	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
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	
Brandon Gleason - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
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	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
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	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
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	
Robert Ganley - Long Island Power Authority - 1	
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	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
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	
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	

Patricia Boody - Lakeland Electric - 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	
Teresa Cantwell - Lower Colorado River Authority - 5	
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	
William Sanders - Lower Colorado River Authority - 1	
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	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
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	
Eric Ruskamp - Lincoln Electric System - 6	
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	
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	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
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	
Pam Feuerstein - Intermountain REA - 3 - 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	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

The changes do clarify that responsible entities must have a process to determine what is an attempt to compromise and provide notification as stated in Requirement R1 Part 1.2 and Requirement R4 Part 4.2. However, please see Texas RE's concern with Responsible Entities developing their own processes in #2.

Given Texas RE's proposed changes to the definitions as described in #1, the reporting timelines in Part 4.2 should be changed to:

-
  - One hour after the determination of a Cyber Security Incident that compromised or disrupted
    - Electronic Access Control or Monitoring Systems.
    - Electronic Security Perimeter(s); or
    - A BES Cyber System; or
  - By the end of the next calendar day after determination of a Cyber Security Incident that **was an attempt to compromise** or disrupt:
    - Electronic Security Perimeter(s); or
    - A BES Cyber System; or

- Electronic Access Control or Monitoring Systems.

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 our response to Question 1. We agree with the concept, but it will require further definition of key terms detailed above to allow Registered Entities the opportunity to meet the Standard in a clear and measurable way.

As for the language of R4, itself, Southern Company suggests the following edits to clarify the scope and applicability that is based on the revised definitions proposed under Q1:

R4: Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC)1, or their successors, of a Reportable Attempted Cyber Security Incident ***or*** *a Reportable Cyber Security Incident.*

For Section 4.2:

After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines:

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

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

Part 4.2 stands on its own. Notification is part of "respond" in Part 1.1 and does not need Part 1.2. Part 4.2 should be clarified so show that all events that meet the definition of "Cyber Security Incident" are reportable, but that only actual compromise or disruption is reportable within one hour.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF

Answer	No
Document Name	

Comment

Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

Comments: Request clarifications on the measures and evidence needed to satisfy the requirement.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1

Answer	No
Document Name	

Comment

Without a NERC defined term for reportable attempted cyber security incidents, entities are left by themselves to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. This could lead to significant inconsistencies among different entities, and the compliance performance measures among different entities could be significantly different.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

See previous comment.

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

“Attempts” have been a part of the definition for a Cyber Security Incident for more than a decade. MEC will not support a process to define “attempts.” Industry has already been identifying attempts for years. Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity’s existing program(s). Every additional change in the terms or Parts creates additional work for Entity’s to revise, implement and retrain.

Further, see the last question for comments on Requirement 4 and its Parts. There are not questions for Requirement 4 in this comment form.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No

Document Name	
Comment	
N&ST agrees that an actual compromise of an ESP or an applicable system should be distinguished from an (unsuccessful) attempt and that it is reasonable to define different reporting time frames for each type of Cyber Security Incident. However, N&ST objects to the use of the word, “only” (as in “Only an attempt...”), as it implies triviality (N&ST also recommends eliminating the definition of “Reportable Cyber Security Incident” as per our response to Question 1). Suggested re-wording for R1 Part 1.2: “Determine whether an identified Cyber Security Incident was an attempt to compromise an ESP or an applicable system or actually compromised or disrupted an ESP or an applicable system.” Suggested re-wording for R4 Part 4.2 “bullets:” (1st) “One hour after a determination that a Cyber Security Incident was an actual compromise or disruption of an ESP or an applicable system.” (2nd) “By the end of the next calendar day after a determination that a Cyber Security Incident was an unsuccessful attempt to compromise or disrupt an ESP or an applicable system.”	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	No
Document Name	
Comment	
Please note that even thought I agree with the flexibility to establish my own criteria, I believe that this flexibility will be addressed in a future NOPR as all applicable Entities will have different criteria of what an attempt to compromise is.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
NV Energy would like to reiterate that “Attempts” have been a part of the definition for a Cyber Security Incident for more than a decade. NV Energy does not support a process to define “attempts.” Industry has already been identifying attempts for years. Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity’s existing program(s). Every additional change in the terms or Parts creates additional work for Entity’s to revise, implement and retrain.	
Likes 0	

Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment

: We disagree with the changes made to Requirement R1, part 1.2.1, which addresses the entity's responsibilities to, "Establish criteria to evaluate **and define** attempts to compromise;"

Recommend remove the term "define," and keep the established scope per NERC, CIP & FERC as: ...

The language would have to be so ubiquitous to cover changes in technologies and encapsulate outlying behavior, that any documented process would be outmoded – and in CONSTANT revisions.

R1.1. already has a criteria to identify the attempts. R.1.1 - One or more processes to identify, classify, and respond to Cyber Security Incidents.)

No - For part 1.2.1, removing "define" allows the entity more flexibility to scope attempts to compromise into their criteria for evaluating the Cyber Security Incident.

R1.2 - One or more processes to: Use: "Respond"?

1.2.1 Establish criteria to evaluate and define attempts to compromise;

1.2.2 Determine if an identified Cyber Security Incident is:

{C}· A Reportable Cyber Security Incident or

{C}· Only an attempt to compromise one or more systems identified in the "Applicable Systems" column identified for this Part;

1.2.3 Provide notification per as specified in Requirement R4 of this Standard.

"**Attempts**" have been a part of the definition for a Cyber Security Incident for more than a decade. PAC will not support a process to define "attempts." Industry has already been identifying attempts for years. Part 1.2 should be changed as little as necessary to accomplish the directive and require the least revisions to each Responsible Entity's existing program(s). Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain. Per our comments on question 1, we recommend incorporating the FERC directive for "attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)" in the Reportable Cyber Security Incident definition. Part 1.2 would retain "One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident." The rest of existing Part 1.2 would be deleted.

Further, we disagree with the proposed Part 1.2 to include any reference to "provide notification per Requirement R4." This recreates a cross-reference between two requirements and potential double jeopardy for noncompliance. Part 1.2 should have NO reference to reporting.

Additionally, **we disagree with the proposed language changes in the Requirements column for Parts 2.2. and 2.3** With our proposed changes from question 1 and this question, Parts 2.2 and 2.3 should only be modified in the Applicable Systems column. There is no question in the comment form for Part 2.2 or 2.3

each Responsible Entity's existing program(s). Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain. Per our comments on question 1, we recommend incorporating the FERC directive for "attempt to compromise, a responsible entity's

Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS)" in the Reportable Cyber Security Incident definition. Part 1.2 would retain "One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident." The rest of existing Part 1.2 would be deleted.

Further, we disagree with the proposed Part 1.2 to include any reference to "provide notification per Requirement R4." This recreates a cross-reference between two requirements and potential double jeopardy for noncompliance. Part 1.2 should have NO reference to reporting.

Additionally, **we disagree with the proposed language changes in the Requirements column for Parts 2.2. and 2.3** With our proposed changes from question 1 and this question, Parts 2.2 and 2.3 should only be modified in the Applicable Systems column. There is no question in the comment form for Part 2.2 or 2.3

{C}1. Do the changes clarify that the Responsible Entity **must have a process to determine** what is an **attempt** to compromise and provide notification as stated **in Requirement R1 Part 1.2 and Requirement R4 Part 4.2**? Please explain and provide comments.

{C}{C}{C} Yes

{C}{C} No

Comments: We disagree that the changes clearly, or need to clarify, based on the following;

R1.1 lays out the criteria to identify Cyber Security Incidents (***which by definition includes attempts***) - One or more processes to identify, classify, and respond to Cyber Security Incidents.)

They include compromises and attempts to compromise. Remove the language, "**and define**…" as stated in: 1.2.1 Establish criteria to evaluate **and define** attempts to compromise; The requirement as stated is too restrictive and would require too many itemizations and feverish revisions as methods and technolies are developed. – uggest to utilize the term and process of 'evaluation' as stated in the R.1. : " identify, classify, and respond" measures. Recommend removal of R.1.2.1, and stick with R.1.1. The scope and intent are included in R.1.1.

PAC will not support a process to define "attempts." **Industry has been identifying attempts for years.** Part 1.2 should be changed to accomplish the FERC directive, and require the least revisions to each Responsible Entity's existing program(s). Every additional change in the terms, or Parts, creates additional work for Entity's to revise, implement and retrain.

Further, see question #10, for comments on Requirement 4, and its Parts. **There are not questions for Requirement 4 in this comment form**:

There are no questions to provide comments on Requirement 4 or its Parts. We do not support these as proposed. With our recommendations in questions 1 and 2, R4 only needs to refer to Reportable Cyber Security Incidents. It does not need to include "a Cyber Security Indicent that was only an attempt to compromise a system identified in the "Applicable Systems" column. This phrase could be deleted.

Suggest change to the following:

"was only an attempt to compromise an identified system applicable system identified in the "Applicable Systems" column for this Part." As identified in R.1.2.2:

{C}· Only an attempt to compromise one or more systems identified in the "Applicable Systems" column identified for this Part;

Review for redundancies: These are defined in scope in the 'Applicable Systems' in Column One of the Standard.

Likes 0	
Dislikes 0	

Response

4. 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? Please provide comments and an alternate approach to addressing the directive, if possible.

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

Answer	Yes
Document Name	

Comment

CenterPoint Energy agrees with the addition of EACMS to the Applicable Systems. Additionally, the Company suggest that entities be allowed to restrict indications of compromise or attempt to compromise to the capability of the EACMS.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

FERC Order 848, ¶ 54 states, “With regard to identifying EACMS for reporting purposes, NERC’s reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide.” We agree with adding “and their associated” EACMS” to the Applicable Systems columns in the Parts. We thank SDT for ensuring these changes keep low impact out of scope for reporting.

Likes 0	
Dislikes 0	

Response

Renee Leidel - Dairyland Power Cooperative - 1

Answer	Yes
Document Name	

Comment

Yes, but I think it should be further qualified to only those systems involved in controlling access. EACMS currently includes systems that may only be for monitoring security that Project 2016-02 would classifiy as EAMS. It seems the intention of adding “EACMS” to the standard here is to target

reporting of what Project 2016-02 calls “EACS” systems. Will this new requirement unqualified be a barrier to utilizing external services related to monitoring access?	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Adding EACMS as CIP-008 applicable makes sense to improve the BES security posture. If the systems controlling access and monitoring a BCS are under attack, response and notification should be required.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
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	Yes
Document Name	
Comment	

We agree with adding “and their associated” EACMS” to the Applicable Systems columns in the Parts. We thank SDT for ensuring these changes keep low impact out of scope for reporting.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 6

Answer	Yes
Document Name	

Comment

LES anticipates this matter will be "cleaned up" in the virtualization project, within this project the SDT is proposing to seperate EACMS into EACS and EAMS.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	Yes
Document Name	

Comment

In addition, PCAs should be included in the Applicable Systems column for requirements and in the definitions for Cyber Security Incident and Reportable Cyber Security Incidents due to their association with BES Cyber Systems and potential for revealing malicious activity directed at the BPS.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	Yes
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Tommy Drea - Dairyland Power Cooperative - 5

Answer	Yes
Document Name	

Comment

Yes, but I think it should be further qualified to only those systems involved in controlling access. EACMS currently includes systems that may only be for monitoring security that Project 2016-02 would classifiy as EAMS. It seems the intention of adding “EACMS” to the standard here is to target reporting of what Project 2016-02 calls “EACS” systems. Will this new requirement unqualified be a barrier to utilizing external services related to monitoring access?

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

Seattle City Light understands the difficulty faced by the SDT regarding EACMS and FERC Order No. 848. We cannot identify a better alternative and reluctantly agree with the proposed approach.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	Yes
Document Name	

Comment

Concur with EEI comments	
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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by NRECA	
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	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
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	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 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 - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
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	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
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	
Chris Scanlon - Exelon - 1	
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	
Tho Tran - Omaha Public Power District - 1 - Texas RE	
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	
Nicholas Lauriat - Network and Security Technologies - 1	
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	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
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	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 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	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
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	
William Sanders - Lower Colorado River Authority - 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	
Teresa Cantwell - Lower Colorado River Authority - 5	
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	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
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	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
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	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 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	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Robert Ganley - Long Island Power Authority - 1	
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	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Please see Texas RE's response to #1 regarding including ESPs as applicable systems.	
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 asserts that the language, as proposed, DOES extend the scope into CIP-003 and low impact BES Cyber Systems. The currently approved definition of "Reportable Cyber Security Incident" has a threshold of actually compromising or disrupting a reliability task of the functional entity. With the SDT's proposed changes to the definition and its use in CIP-003, what is reportable at assets containing lows could now be any compromise or disruption of any BES Cyber System, any "logical borders surrounding a network to which BES Cyber Systems are connected using a routable protocol", any "physical borders in which BES Cyber Assets reside…" or any EACMS. It appears the SDT attempts to limit the CIP-003 scope expansion with the use of the nested "Cyber Security Incident" definition. The EACMS are scoped to high and medium in the CSI definition and then uses it as the basis of the Reportable CSI definition. Southern asserts that the ESP (and PSP) term in the CSI definition is not likewise scoped and leaves an ambiguity. Simply because no requirements in CIP-005 or CIP-006 apply at a site that only contains low impact systems does not mean that a logical or a physical border does not exist at the location that meets these definitions. Therefore, if a firewall at a 100kV "low only" substation is plugged into a UPS and the UPS "suspiciously" powers off, then both an ESP (the logical border…) and an EACMS is disrupted at that low	

substation. It seems to be reportable under one sub-bullet (ESP) but not another (EACMS) and therefore becomes a reportable incident under CIP-003 (CIP-008's scoping language has no bearing on this situation).

Southern suggests this ambiguity can be removed by moving the qualifier for high and medium to earlier in the definition, as suggested under Southern's proposed modifications presented in Q1, and by also specifying high and medium impact-associated EACMS under the Reportable Cyber Security Incident definition:

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

- For high or medium impact BES Cyber Systems, compromised, or was an attempt to compromise, (1) the ESP, (2) the PSP, or (3) the associated EACMS; or
- Disrupted, or was an attempt to disrupt, the operation of a BES Cyber System

Reportable Attempted Cyber Security Incident – a *confirmed* malicious act that was determined by the Responsible Entity to be:

- An attempt to compromise the ESP of a high or medium impact BCS; or
- 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 the ESP of a high or medium impact BCS; or
- Disrupted the operation of a BES Cyber System, *or high or medium impact-associated EACMS*

In fact, Southern suggests that "Electronic Security Perimeter" could be deleted from the definition now that EACMS has been added, as the two appear redundant. Would not any attempt to compromise or disrupt "the logical border…" occur at an EACMS? Southern provides this as a point of discussion only.

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

EACMS should not be included. Systems that only perform the 'Monitoring' portion of an EACMS should not be included due to the minimal risk they pose compromising the BES. TVA has taken an enterprise approach to Cybersecurity monitoring and the system is implemented and designed to be isolated from the BES components in such a manner that a compromise of the system can in no way impact the BES.

Likes 0	
Dislikes 0	

Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	No
Document Name	
Comment	
I marked No here because of my comments in question 1 above. Those thoughts regarding the SDT 2016-002 are applicable here as well.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	No
Document Name	
Comment	
POPUD is afraid that the way this is addressed will cause ambiguity and confusion for low impact BES Cyber Systems, and unnecessary reporting of minor issues invoving low impact assets.	
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.	
Likes 0	
Dislikes 0	
Response	

5. Do you agree with reporting timeframes included Requirement R4 Part 4.2 and Part 4.3 which include an increase in reporting timeframe from 5 to 7 calendar days in Part 4.3? Please explain and provide comments.

Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	Yes
Document Name	

Comment

Xcel Energy believes that additional clarity should be provided in Requirement 4.2 so that it is stated that notifications of a Reportable Cyber Security Incident must be made one hour after its determination, even if it was already reported as an attempt. The upgrade from an attempt to an actual compromise requires a new notification within 24 hours per Requirement 4.2, not just an update.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

Southern Company supports the “update timeframe” in R4.4 to be set at 7 calendar days which will facilitate regular and timely reporting for issues of an extended duration. This timeframe 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

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

Answer	Yes
Document Name	

Comment

AECI supports comments provided by NRECA

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	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
While AZPS appreciates the change from 5 to 7 calendar days, as noted in our previous comments, a continual updating of information every 7 days may result in inaccurate information and an undue burden on resources. Therefore, it is recommended that an initial notification is made and then a final update at the completion of a Cyber Security Incident.	
Likes 0	
Dislikes 0	
Response	
Thomas Breene - WEC Energy Group, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Concur with EEI comments. Aditionally, while WEC Energy Group supports the proposed reporting timeframes, we recognize the need for a CIP Exceptional Circumstances clause to be added to Requirement R4 to manage the situation where the reporting timeframe cannot be met due to declared CEC.	
Likes 0	

Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light appreciates the additional time allowed for follow-on reporting, which better accommodates uncommon situations that, nonetheless, occur with some regularity, such as holiday season, vacations, and operational emergencies.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	Yes
Document Name	
Comment	
We appreciate that the SDT has provided additional time for the updates to the original notification; however, we are not convinced that the timeframe is appropriate for all situations. The requirement may add additional administrative burden for tracking the periodic updates and may not add commensurate reliability benefits.	
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	

We appreciate that the SDT has provided additional time for the updates to the original notification; however, we are not convinced that the timeframe is appropriate for all situations. The requirement may add additional administrative burden for tracking the periodic updates and may not add commensurate reliability benefits

Likes 0	
Dislikes 0	

Response

Matthew Beilfuss - WEC Energy Group, Inc. - 4

Answer	Yes
Document Name	

Comment

While WEC Energy Group supports the proposed reporting timeframes, we recognize the need for a CIP Exceptional Circumstances clause to be added to Requirement R4 to manage the situation where the reporting timeframe cannot be met due to declared CEC.

Likes 0	
Dislikes 0	

Response

Michael Buyce - City Utilities of Springfield, Missouri - 1

Answer	Yes
Document Name	

Comment

Referring to the “Applicable Systems” column in the “Requirements” column may be redundant. A suggestion for the language in the second bullet for Part 4.2 is: “By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise (as defined in Part 1.2.1) one or more applicable systems.”

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	Yes
Document Name	

Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Yes we agree 7 is more suitable timeframe because it allows the organization to be more thorough in analysis performance, evidence gathering and fact finding, before reporting back to the region.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	

NV Energy agrees with the additional days for reporting additional information to E-ISAC and NCCIC.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	Yes
Document Name	

Comment

There should be a consistent reporting timeframe for all, R4.2 & R4.3. A SEVEN calendar day reporting timeframe allows an entity a more reasonable timeframe to report, and subsuqent follow-up reporting. FERC Order 848, ¶ 53 states, "…NERC should have the flexibility to establish an appropriate reporting threshold." This increase supports this.

Likes 0	
Dislikes 0	

Response

Constantin Chitescu - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

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	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
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	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
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	
Robert Ganley - Long Island Power Authority - 1	
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	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
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	

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	
Steven Rueckert - Western Electricity Coordinating Council - 10	
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	
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	
Teresa Cantwell - Lower Colorado River Authority - 5	
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	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
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	
Eric Smith - NaturEner USA, LLC - 5	
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	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
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	
Eric Ruskamp - Lincoln Electric System - 6	
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	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
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	
Nicholas Lauriat - Network and Security Technologies - 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	
David Jendras - Ameren - Ameren Services - 3	
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	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

ERCOT requests that CIP Exceptional Circumstances be added to Part 4.2. As ERCOT noted in its comments on the last version, responsible entities need to focus on reliability and restoration without the burden of meeting a reporting deadline during these activities. Alternatively, this could be added to the overarching Requirement R4. In the SDT's consideration of comments for the last version, the SDT noted that the 2016-02 SDT would address this. ERCOT requests that the 2018-02 SDT address this in in the new requirement being developed since the new reporting timelines will be subject to the implementation plan for CIP-008-6. Proposed language: Part 4.2, "After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines, except during CIP Exceptional Circumstances:".

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

While we agree with the increase in the reporting timeframe from 5 to 7 calendar days in Part 4.3, we still have concerns with the reporting timeframes in Part 4.2. We strongly encourage NERC and the SDT to reconsider requiring each Responsible Entity (RE) to report to two different agencies (E-ISAC and NCCIC). 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 Part 4.2 requirement to: *"**Two hours** after the determination of a Reportable Cyber Security Incident. **48 hours** after determination that a Cyber Security Incident was only an attempt..."* 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 NCCIC (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, especially in times of crisis when there may be longer delays/higher volume in contacting these agencies. This updated requirement is doubling the reporting requirements of CIP-008-5 while keeping the same one hour reporting timeframe for Reportable Cyber Security Incidents.

Likes 0	
Dislikes 0	

Response

Jeanne Kurzynowski - Consumers Energy Co. - 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/regulations 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	

Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	No
Document Name	
Comment	
Tacoma Power appreciates that the SDT has provided additional time for the updates to the original notification; however, we are not convinced that the timeframe is appropriate for all situations. The requirement will add additional administrative burden for tracking the periodic updates and may not add commensurate reliability benefits.	
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	
Amelia Sawyer Anderson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes the timeframes are confusing and could result in unintended actions such as shortened investigations and minimal reporting. Requirements with timeframes are often most violated unintentionally. This could especially be the case during a high-stress incident response scenario. Suspicious system behavior could take a long time to understand and resolve. Entities should not be penalized for not reporting new information gained over a long timeframe.	
Likes 0	
Dislikes 0	
Response	

6. Do you agree with the SDT's decision to give the responsible entity the flexibility to determine notification methods in their process? Please explain and provide comments.

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

Answer	Yes
Document Name	

Comment

Southern Company notes that the CIP-008-6 Standard language has changed for notification methods, yet the Technical Rationale, in the section labeled "**Methods for Submitting Notifications",** references "submit notification using any *approved* method supported by E-ISAC and NCCIC". Southern Company requests that this be changed to read, "submit notification using any method supported by E-ISAC and NCCIC." The use of "approved" implies an approval process that is not addressed in the current Standard language or draft Implementation Guidance.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

While we agree with the SDT's decision to provide flexibility in notification methods, with regards to reporting to two independent agencies (E-ISAC and NCCIC), and potentially a third agency if checkbox number 10 under the schedule 1 alert criteria for DOE OE-417 reporting applies, we disagree that this is a cost effective and efficient use of Responsible Entities (REs) time and resources, especially during an emergency event/crisis situation. We ask that NERC and the SDT consider coordinating with E-ISAC and NCCIC to implement an electronic reporting form for ease of initial reporting, updating, and tracking that has the capability, upon submission, to automatically route the data to both agencies. This would save REs the undue burden of submitting twice (or thrice) and potentially encountering discrepancies between the two/three 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 NCCIC. Reporting should be modeled after DOE OE-417 reporting form where one agency's form provides a flag/check option to coordinate with the other one so that the RE only needs to report once. This would cover the RE's responsibility to report to both agencies when necessary, but ensures E-ISAC and NCCIC are coordinating any response. It is our understanding that E-ISAC already works closely with NCCIC per the below cited references:

- Per DHS' website under the expanded section, Information Sharing and Analysis Centers [ISACs], "*Sector-specific Information Sharing and Analysis Centers (ISACs) are non-profit, member-driven organizations formed by critical infrastructure owners and* ***operators to share information between government and industry****. While the* ***NCCIC works in close coordination with all of the ISACs****, a few critical infrastructure sectors maintain a consistent presence within the NCCIC*."

- In addition, in Presidential Decision Directive 63 under President Clinton in the section Annex A: Structure and Organization under the description of Information Sharing and Analysis Center (ISAC), it states, "***Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC****. The center could* ***also gather, analyze and disseminate information from the NIPC for further distribution to the private sector****. While crucial to a successful*

government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government."

- Per the FEMA website, "*In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters.*"

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	Yes
Document Name	

Comment

NV Energy wants to commend the SDT for listening to industry comment and removing the form for communication, and allowing Entities the flexibility to determine notification. We would also request that any upcoming drafts not include this Appendix.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

EEI supports the SDT's decision to provide responsible entities the flexibility to determine the most effective notification method for submitting Cyber Security Incident information to the E-ISAC and ICS-CERT within their processes.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment	
Ameren Agrees with and supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST supports giving Responsible Entities this flexibility but is concerned about the possibility that the recipients of these notifications may be unwilling to accommodate a multitude of different notification methods and report formats. N&ST recommends that NERC, the Regions, the E-ISAC and the DHS work cooperatively to define a SINGLE report template that can be used system-wide to reduce administrative overhead.	
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	Yes
Document Name	

Comment	
We thank the SDT for responding to comments and eliminating the proposed appendix in the standard. Do not put it back in the standard.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
The flexibility that this change provides will allow entities to modify reporting formats as technology, regulatory requirements, and possibly organizations being reported to change over time.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

Recommend the SDT consider the addition of identifying potential notification methods to the Part 1.2 measures to ensure these details are not overlooked when entities develope processes.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

Seattle City Light generally is agnostic to reporting method, but would prefer that if duplicate reporting is required, both reports can be made by the same method and format. See also discussion in question 9.

Likes 0	
Dislikes 0	

Response

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	Yes
Document Name	

Comment

Concur with EEI comments

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	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	
It is not clear how auditors, or enforcement staff, will be restrained from exercising subjective judgement of sufficiency regarding the entites' notification methods and process.	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
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	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
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	
Constantin Chitescu - Ontario Power Generation Inc. - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
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	
Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
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	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
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	
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	
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	
Eric Ruskamp - Lincoln Electric System - 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	

Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
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	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 5	
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	
Andrea Barclay - Georgia System Operations Corporation - 4	
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	
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	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Vivian Vo - APS - Arizona Public Service Co. - 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	
Tim Womack - Puget Sound Energy, Inc. - 3	
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	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Jackson - U.S. Bureau of Reclamation - 1	
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	

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format, as the same event may need to be reported to multiple agencies.	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
Answer	No

Document Name	
Comment	
I am not sure of the rationale behind removing 4.2 from the standard. It seemed to cover nearly any type of method of notification. So if by that it is intended to provide flexibility I guess that the notification process should be required to be noted as part of the plan so that it can be traced in the event of an incident.	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	No
Document Name	
Comment	
It is not clear what the SDT means with the language, "*flexibility to determine notification methods in their process.*" Is this referring to language in the R 4.2 that was deleted in this version? Otherwise, the "flexibility" is not included. The measures for the new R 4.2 state just a single measure: *Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC*.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
Comments: There should be a standardized reporting form which gathers all required attributes and necessary information that is automatically sent to multiple agencies once submitted (e.g single portal which distributes to E-ISAC and NCCIC).	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	

Answer	No
Document Name	
Comment	
One of the four elements outlined by FERC was to improve the quality of reporting and allow for ease of comparison. In order to collect consistent data a framework for reporting is needed.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	No
Document Name	
Comment	
We are unsure what the SDT considers the “flexibility to determine notification methods in their process”. Is this referring to language in the 4.2 that was deleted in this version? Otherwise, we do not see flexibility included. The measures for the new 4.2 state just a single measure: Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format, as the same event may need to be reported to multiple agencies.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	

Answer	No
Document Name	
Comment	
Comments: A formal template should be provided to industry to ensure consistent information is provided.	
Likes 0	
Dislikes 0	
Response	

7. Based on feedback the SDT has adjusted the Implementation Plan timeframe from 12 to 18 months. In the Consideration of Comments Summary Report the SDT justified this change. Do you support the rationale to move to an 18-month Implementation Plan? Please explain and provide comments.

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

Answer	Yes
Document Name	

Comment

AECI supports comments provided by NRECA

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

Thomas Breene - WEC Energy Group, Inc. - 3

Answer	Yes
Document Name	

Comment

Concur with EEI comments

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light appreciates the additional time allowed to develop, implement, and socialize the revised incident response and reporting requirements.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
What is the SDT's intent for the initial performance of Part 2.1? Recommend the SDT address Part 2.1 in the Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	Yes
Document Name	
Comment	
We support the extended implementation timeframe.	
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	
We support the extended implementation timeframe.	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST supports this change. N&ST believes it may require considerable amounts of time and effort for Responsible Entities to define, test and, as necessary, adjust criteria and metrics that they will use to distinguish “noise” from serious attempts to compromise their operational cyber infrastructures. It may also take considerable amounts of time and effort to define and, in some instances, assign staff to reporting functions.	
Likes 0	
Dislikes 0	
Response	

Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
David Jendras - Ameren - Ameren Services - 3	
Answer	Yes
Document Name	
Comment	
Ameren Agrees with and supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
We agree with the adjusted 18 month timeframe as it was necessary to assist RE's in setting up its documented approach for classifying and reporting attempts. The time is also needed to adjust internal processes, provide training to necessary staff, and implement the changes to reporting.	
Likes 0	
Dislikes 0	
Response	
Mark Gray - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
EEI supports the SDT’s decision to move to an 18-month Implementation Plan in response to Industry comments.	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
The additional time for implementation is well needed given the additional administrative burden on Entitie's to meet this Reliability Standard.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
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	
Lynn Goldstein - PNM Resources - Public Service Company of New Mexico - 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	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
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	
Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
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	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
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	
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	
Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
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	

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	
Teresa Cantwell - Lower Colorado River Authority - 5	
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	
William Sanders - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

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	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
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	
James Anderson - CMS Energy - Consumers Energy Company - 1	
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	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
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	
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	
Darnez Gresham - Darnez Gresham On Behalf of: Annette Johnston, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
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	
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	
Tho Tran - Omaha Public Power District - 1 - Texas RE	
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	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
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	
larry brusseau - Corn Belt Power Cooperative - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
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	
Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
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	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
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 believes that due to the program changes required, 24 months is necessary. Given that these changes go from reporting known, clearly defined, objective events that have caused actual impact, to a very subjective “attempts to compromise” that are not easily and quickly determined, nor lend themselves to automated detection without flooding the intended recipients, it will require Responsible Entities to deploy additional resources, modify many existing security processes, potentially implement additional security controls and systems, and coordinate these changes across large enterprises. Therefore, 24 months is a more reasonable timeframe for successful implementation of the necessary changes.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	

For small to medium sized RE's, a significant lift is required to staff the required positions, train/retrain, implement the technologies and create cross functional processes to meet the newly revised standards. A 24 month Implementation Plan is recommended.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

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

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Tommy Drea - Dairyland Power Cooperative - 5

Answer	No
Document Name	

Comment

These changes should not be a significant effort to implement and 12 months seem sufficient to update program documentation and train SMEs of the changes. This standard would need to be revised again if Project 2016-02 is implemented and the definition for EACMS changes. If the implementation timeline is extended too far, a conflict could add more work.	
Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 1	
Answer	No
Document Name	
Comment	
These changes should not be a significant effort to implement and 12 months seem sufficient to update program documentation and train SMEs of the changes. This standard would need to be revised again if Project 2016-02 is implemented and the definition for EACMS changes. If the implementation timeline is extended too far, a conflict could add more work.	
Likes 0	
Dislikes 0	
Response	

8. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R1 and R4? Please explain and provide comments.

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

Answer	Yes
Document Name	

Comment

While EEI generally agrees with the Violation Severity Levels, we suggest the SDT consider making the following minor modification to the phrase “only an attempt to compromise” to “an attempt to compromise”. Although we understand the SDT’s reasoning for adding “only” to the phrase, we believe it offer little additional clarity yet does have the potential of adding confusion to the phrase. Moreover, within Requirement 1, Subpart 1.2.1 entities are required to define “attempts to compromise”.

Affected VSL:

- R1, Severe VSL
- R2, Severe VSL
- R4, Lower VSL, Moderate VSL

Likes 0	
Dislikes 0	

Response

Renee Leidel - Dairyland Power Cooperative - 1

Answer	Yes
Document Name	

Comment

Generally yes, but R4 appears to have an error. The same text “The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident (R4)” appears under both High VSL and Severe VSL columns.

Likes 0	
Dislikes 0	

Response

David Jendras - Ameren - Ameren Services - 3

Answer	Yes
Document Name	

Comment

Ameren Agrees with and supports EEI Comments	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Generally yes, but R4 appears to have an error. The same text “The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident (R4)” appears under both High VSL and Severe VSL columns.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
BPA thanks the SDT for making the modifications.	

Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	Yes
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	
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	

Brandon Gleason - Electric Reliability Council of Texas, 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	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
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	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	

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	
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	
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	
Eric Ruskamp - Lincoln Electric System - 6	
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	
Eric Smith - NaturEner USA, LLC - 5	
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	
Kjersti Drott - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Michael Buyce - City Utilities of Springfield, Missouri - 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	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 5	
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	
Andrea Barclay - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
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	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
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	
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	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Vivian Vo - APS - Arizona Public Service Co. - 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	
Tim Womack - Puget Sound Energy, Inc. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	
Due to shorted balloting period Xcel Energy was not able to evaluate the modifications to VRF or VSLs.	
Likes 0	
Dislikes 0	

Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	
Document Name	
Comment	
No opinion.	
Likes 0	
Dislikes 0	
Response	
Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations	
Answer	No
Document Name	
Comment	
As stated above, any auditor can take issue with a Responsible Entity's "criteria to evaluate and define attempts to compromise" as it is impossible to define with ever changing threats. Because an auditor can interpret this, a High VSL to R1 is not reasonable. We recommend low and moderate for "attempts".	
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 does not support the VRFs and VSLs for Requirement R1 and R4 and consider that they do not appropriately outline the true minimal risk and potential severity to the BES, as written. Given the risk-based nature of NERC's CMEP program, Southern requests the addition of Lower and Moderate VSLs under Requirement R1, and language detailing truly tiered severity levels. Examples for Requirement R1: Lower VLS:	

The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to provide notification per Requirement R4. (1.2)

Moderate VSL:

The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Attempted Cyber Security Incidents.

High VLS:

The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents.

Examples for Requirement R4:

Lower VLS:

The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Attempted Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

For R1, we believe that failure to include processes to identify Cyber Security Incidents that were only an attempt to compromise an applicable system should be at a lower VSL than failing to include processes to identify Reportable Cyber Security Incidents (RCSI) as there is a clear difference in a RCSI's potential impact to the BES versus only an attempt (which would not have an actual impact to the BES). We believe that all failures related only to attempts should be classified as "Lower VSL" based on their lack of actual impact to the BES. Similarly, for R4, the same logic should apply. A failure to notify an information sharing organization of an unsuccessful attempted Cyber Security Incident should not result in a Moderate VSL, but rather a Lower VSL based on actual impact to the BES (or lack thereof). Furthermore, if a Responsible Entity only notified one agency, this should be considered nothing higher than a Lower VSL as the incident was still reported and should have been shared between agencies.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee

Answer	No

Document Name	
Comment	
For R4, there seems to be duplication of criteria for Severe and High VSL regarding the following: “The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4).” Which shows up in both columns (Severe and High VSL). Otherwise, the VSL language seems appropriate.	
Likes 0	
Dislikes 0	
Response	
Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Salsbury - Berkshire Hathaway - NV Energy - 5	
Answer	No
Document Name	
Comment	
Given our comments on previous items, NV Energy cannot approve the currently drafted VRF and VSLs, as our comments on revisions would require changes be made to the VRFs and VSLs to reflect NV Energy's recommendations.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	

Answer	No
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
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	
We do not agree with Requirements and Parts as proposed. The VRFs and VSLs have to be revised too.	
Likes 0	
Dislikes 0	
Response	
James Anderson - CMS Energy - Consumers Energy Company - 1	
Answer	No
Document Name	
Comment	
The current proposed requirements still need to be refined by the Standard Drafting Team. And the VRF and VSL should be updated accordingly.	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2	
Answer	No
Document Name	

Comment	
While we don't agree, we have found it doesn't merit the effort to provide alternatives.	
Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
The current proposed requirements still need to be refined by the Standard Drafting Team. And the VRF and VSL should be updated accordingly.	
Likes 0	
Dislikes 0	
Response	
Robert Ganley - Long Island Power Authority - 1	
Answer	No
Document Name	
Comment	
Comments: Until the standard language is more formalized the Violation Risk Factors or Violation Severity Levels may not accurately reflect the risks.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

For R4, there seems to be duplication of criteria for Severe and High VSL regarding the following:

“The Responsible Entity failed to notify E-ISAC or NCCIC, or their successors, of a Reportable Cyber Security Incident. (R4).”

Which shows up in both columns (Severe and High VSL).

Otherwise, the VSL language seems appropriate.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

Answer	No
Document Name	

Comment

Reclamation does not agree with the High VSL for R4. Reclamation recommends 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 Requirement R4 Part 4.3.

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 Requirement R4 Part 4.3 but failed to update E-ISAC or DHS, or their successors, within the timeframe included in Requirement R4 Part 4.4.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	No
Document Name	

Comment
R1 Severe VSL seems to be extreme for an admisitrative failure to include "only and attempt to compromise". R1 High VSL seems to be extreem for the administrave failure to have a process to identify criteria to define attempts to compromise. POPUD forsees arguments between the entity the auditors and enforcement staff over the sufficiency of these sections. We are aware of instances where auditors have decided that an issue was techicallyaddressed, but it wasn't addressed to their satisfaction. Most recently there is a discussion of the sufficiency of certain chains and locks used for CIP-014. We would like these issues addressed going forward during Standard development, rather than when the Standards are being enforced.

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 attempted Cyber Security Incident should not result in a severe penalty.

Likes 0	
Dislikes 0	

Response

9. 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

NRG does not have concerns in acheiving these reliability objectives in a cost effective manner; however, this may be challenging for Responsible Entities who have manual processes for evaluation.

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	Yes
Document Name	

Comment

However, the auditors may not agree with the cost effective approach and demand a higher level (best practices) application. This puts smaller entities in jeopardy during audits.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	Yes
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
We appreciate the development of the Implementation Guide and we agree with SDT approach to allow RE's to develop a model based on the analaysis of the current environment and the time to discuss future projections for realistic budgetary stance.	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
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	
Daniel Valle - Daniel Valle On Behalf of: William Winters, Con Ed - Consolidated Edison Co. of New York, 3, 1, 5, 6; - Daniel Valle	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Black Hills Corporation - 1,3,5,6 - WECC	
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	
Mike Smith - Manitoba Hydro - 1, Group Name Manitoba Hydro	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Vivian Vo - APS - Arizona Public Service Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
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	
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	
Thomas Breene - WEC Energy Group, Inc. - 3	
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	
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	
Teresa Cantwell - Lower Colorado River Authority - 5	
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	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Seth Shoemaker - Muscatine Power and Water - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tommy Drea - Dairyland Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Eric Smith - NaturEner USA, LLC - 5	
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	
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	
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	
David Jendras - Ameren - Ameren Services - 3	
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	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Renee Leidel - Dairyland Power Cooperative - 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	
Kimberly Van Brimer - Southwest Power Pool, Inc. (RTO) - 2 - MRO	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Pam Feuerstein - Intermountain REA - 3 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Todd Bennett - Associated Electric Cooperative, Inc. - 3, Group Name AECI	
Answer	
Document Name	
Comment	
AECI supports comments provided by NRECA	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE does not have comments on this question.	
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 SDT's modifications to provide flexibility, with regards to reporting to two independent agencies (E-ISAC and NCCIC), and potentially a third agency if checkbox number 10 under the schedule 1 alert criteria for DOE OE-417 reporting applies, we disagree that this is a cost effective and efficient use of Responsible Entities (REs) time and resources, especially during an emergency event/crisis situation. We ask that NERC and the SDT consider coordinating with E-ISAC and NCCIC to implement an electronic reporting form for ease of initial reporting, updating, and tracking that has the capability, upon submission, to automatically route the data to both agencies. This would save REs the undue burden of submitting twice (or thrice) and potentially encountering discrepancies between the two/three 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 NCCIC. Reporting should be modeled after DOE OE-417 reporting form where one agency's form provides a flag/check option to coordinate with the other one so that the RE only needs to report once. This would cover the RE's responsibility to report to both agencies when necessary, but ensures E-ISAC and NCCIC are coordinating any response. It is our understanding that E-ISAC already works closely with NCCIC per the below cited references:

- Per DHS' website under the expanded section, Information Sharing and Analysis Centers [ISACs], "*Sector-specific Information Sharing and Analysis Centers (ISACs) are non-profit, member-driven organizations formed by critical infrastructure owners and* ***operators to share information between government and industry****. While the* ***NCCIC works in close coordination with all of the ISACs****, a few critical infrastructure sectors maintain a consistent presence within the NCCIC*."

- In addition in Presidential Decision Directive 63 under President Clinton in the section Annex A: Structure and Organization under the description of Information Sharing and Analysis Center (ISAC), it states, "***Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC****. The center could* ***also gather, analyze and disseminate information from the NIPC for further distribution to the private sector****. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government*."

- Per the FEMA website, "*In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters.*"

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	No
Document Name	

Comment

The new standard ultimately requires Responsible Entities to become cyber security threat hunters rather than relying on the protections required within the CIP standards. There is no reduction in risk to the BES in reporting attempts to compromise. CIP-008-6's new requirements are going to require significant investments in technology and personnel for small and medium sized Regional Entities without an existing 24x7x365 Security Operations Center (SOC). A 24x7x365 SOC, is a multi-million dollar capital investment and a significant operational and maintenance budget burden. At a minimum, a SOC requires six qualified FTE to cover shifts plus, a threat hunter, oversight, compliance reporting, and management. Salaries alone for a small SOC are in excess of $1,000,000. This is just not feasible for a small or medium sized entity. Using a Managed Service Provider for SOC services to reduce cost is also not feasible due to access to BCSI, its inherent requirements, and increased compliance risk.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	

Comment

Including EACMs increases documentation of attempts which makes the requirement onerous for the entities.

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

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

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

With regard to reporting to two independent agencies (E-ISAC and NCCIC), it seems strange to have duplicate reporting. Would it not make sense to avoid such inefficiency by simply reporting to E-ISAC and asking them to forward relevant items to DHS?

Likes 0	
Dislikes 0	

Response

Robert Ganley - Long Island Power Authority - 1

Answer	No
Document Name	

Comment

Comments: Since the standard has been expanded to include “Attempts” the costs will increase incrementally regardless of the flexibility provided.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

Seattle City Light appreciates the efforts of the SDT to provide flexibility in draft CIP-008-6. City Light also appreciates the work of the SDT to respond to industry comments from the first posting, and to provide extensive guidance documentation about the intent of the draft CIP-008 revisions and how the revised requirements might be implemented. For the most part, the revisions provide flexibility to meet reliability objectives in a cost effective manner, and the additional documentation offers reasonable assurance about acceptable means to meet these objectives.

In one area the modifications fall short, that of still requiring double-reporting of Reportable Cyber Security Incidents and attempted incidents to E-ISAC and to DHS NCCIC. This duplication of effort is neither cost effective for an entity nor is it the best use of scare resources during an actual cyber security incident to focus attention on a duplicative task. City Light urges the SDT to coordinate directly with NERC to arrange for E-ISAC to make the reportings to DHS NCCIC. Coordination of reporting is appropriate for E-ISAC both as part of its expanded industry engagement (and expanded budget) and in its central role as an analysis and sharing center, one step removed from the front lines of cyber issues at an entity. City Light understands that such a change might require additional negotiation among FERC, NERC, and E-ISAC, outside of the Standards process, but believes the result to be beneficial, appropriate, and consistent with the intent of FERC Order No. 848.

Likes 0	
Dislikes 0	
Response	
Jeanne Kurzynowski - Consumers Energy Co. - 1,3,4,5 - RF	
Answer	No
Document Name	
Comment	
Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format, as the same event may need to be reported to multiple agencies.	
Likes 0	
Dislikes 0	
Response	
Patricia Boody - Lakeland Electric - 3	
Answer	No
Document Name	
Comment	
We are concerned that the timelines for reporting may create additional administrative burden and cost. In addition, Entities that have an integrated EOP-004/CIP-008 all hazards approach to incident management will have considerable costs and effort to accomplish these changes.	
Likes 0	
Dislikes 0	
Response	
Joe O'Brien - NiSource - Northern Indiana Public Service Co. - 6	
Answer	No
Document Name	
Comment	
Dependent upon what constitutes an “attempt”, additional resources (personnel and/or tools) may be needed to investigate and report on attempted events.	

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	
We are concerned that the timelines for reporting may create additional administrative burden and cost. In addition, Entities that have an integrated EOP-004/CIP-008 all hazards approach to incident management will have considerable costs and effort to accomplish these changes.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rick Applegate - Tacoma Public Utilities (Tacoma, WA) - 6	
Answer	No
Document Name	
Comment	

Tacoma Power is concerned that the timelines for reporting may create additional administrative burden and cost. In addition, Entities that have an integrated EOP-004/CIP-008 all hazards approach to incident management will have to expend significant resources to comply with these changes. There is no evidence that reliability and security benefits will be commensurate with the increased costs.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	No
Document Name	

Comment

See our comments in the next question.

Likes 0	
Dislikes 0	

Response

James Anderson - CMS Energy - Consumers Energy Company - 1

Answer	No
Document Name	

Comment

Please coordinate with EOP-004 and OE-417 regulators for a standardize reporting timeline and reporting format, as the same event may need to be reported to multiple agencies.

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

The directives can be implemented with fewer changes to the Glossary terms and Requirements. Both should be changed as little as necessary to accomplish the directive and require the least revisions to Responsible Entity's existing programs. Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain and produce evidence for compliance monitoring without adding value to security or reliability.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Absent assurances from the appropriate authorities at the E-ISAC and the DHS that Responsible Entities will be able to use one reporting mechanism and one standardized report template for incident reporting, N&ST is concerned that the administrative overhead associated with filing and updating reports could be significant.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	No
Document Name	

Comment
NV Energy cannot make a determination on the implementation for this Standard being done in a cost effective manner given the current draft. Previous comments provided by NV Energy would require changes to the Definitions and Requirement that would support a more cost effective implementation.

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6	
Answer	No
Document Name	

Comment
We do not agree. The directives can be implemented with fewer changes to the Glossary terms and Requirements. Both should be changed as little as necessary to accomplish the directive and require the least revisions to Responsible Entity's existing programs. **Every additional change in the terms or Parts creates additional work for Entity's to revise, implement and retrain and produce evidence for compliance monitoring without adding value to security or reliability, thus is no longer 'cost effective'**.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee	
Answer	No
Document Name	

Comment
With regard to reporting to two independent agencies (E-ISAC and NCCIC), it seems strange to have duplicate reporting. Would it not make sense to avoid such inefficiency by simply reporting to E-ISAC and asking them to forward relevant items to DHS?

Likes 0	
Dislikes 0	

Response

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

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

Answer	
Document Name	

Comment

The diagram in the Implementation guidance (page 6) references capitalized terms for "Attempted", "Compromise" and "Disrupt" which could be confusing to Responsible Entities.

Likes 0	
Dislikes 0	

Response

Jodirah Green - ACES Power Marketing - 6, Group Name ACES Standard Collaborations

Answer	
Document Name	

Comment

Thank you for the opportunity to comment.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

Regarding the Technical Rationale and Justification for Reliability Standard CIP-008-6, ERCOT requests that the historical rationale not be removed from the standard until this document is approved. If the content is removed and the Technical Rationale and Justification for Reliability Standard CIP-008-6 is not approved, valuable historical context for the full standard will disappear.

Regarding the implementation guidance, ERCOT requests that the historical Guidelines and Technical Basis not be removed from the standard until this document is endorsed by the ERO. If the content is removed and the Implementation Guidance for Reliability Standard CIP-008-6 is not endorsed, valuable historical context for the full standard will disappear.

ERCOT also offers the following comments on the Implementation Guidance:

- Page 7, typo correction: “Once this initial notification is made, if all attributes were known, they should have been included in the initial notification and the reporting obligation ends.
- Page 7 concern: It is noted that an entities reporting obligations are met once known information for the three required attributes is reported to E-ISAC and NCCIC. This appears to indicate that entities are non-compliant up to this point. Requirement R4 allows partial reporting while maintaining compliance.
- Page 11 correction: The NERC Functional Model is not contained within Attachment 1 of CIP-002. The NERC Functional Model is a wholly separate document.
- Page 18 type: “Registered Entities are encouraged to explore options and tools designed to that take the guess work out of the process without being so overly prescriptive as to create undue administrative burden or remove needed discretion and professional judgment from the SMEs.”
- Page 18 concern: As noted in response to question 2, ERCOT has concerns with it being up to the Registered Entity to determine what constitutes and ‘attempt to compromise’. ERCOT recommends the SDT use industry-standard guidance to develop a baseline or minimum criteria for the industry.
- Pages 23-35 concern: ERCOT requests that the SDT consider removing the requirement language. This will ensure that the guidance is relevant and applicable beyond the current proposed version of the requirement language.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

With regards to reporting to two independent agencies (E-ISAC and NCCIC), and potentially a third agency if checkbox number 10 under the schedule 1 alert criteria for DOE OE-417 reporting applies, we disagree that this is a cost effective and efficient use of Responsible Entities (REs) time and resources, especially during an emergency event/crisis situation. We ask that NERC and the SDT consider coordinating with E-ISAC and NCCIC to implement an electronic reporting form for ease of initial reporting, updating, and tracking that has the capability, upon submission, to automatically route the data to both agencies. This would save REs the undue burden of submitting twice (or thrice) and potentially encountering discrepancies between the two/three 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 NCCIC. Reporting should be modeled after DOE OE-417 reporting form where one agency’s form provides a flag/check option to coordinate with the other one so that the RE only needs to report once. This would cover the RE’s responsibility to report

to both agencies when necessary, but ensures E-ISAC and NCCIC are coordinating any response. It is our understanding that E-ISAC already works closely with NCCIC per the below cited references:

- Per DHS' website under the expanded section, Information Sharing and Analysis Centers [ISACs], "*Sector-specific Information Sharing and Analysis Centers (ISACs) are non-profit, member-driven organizations formed by critical infrastructure owners and* ***operators to share information between government and industry****. While the* ***NCCIC works in close coordination with all of the ISACs****, a few critical infrastructure sectors maintain a consistent presence within the NCCIC*."
  In addition in Presidential Decision Directive 63 under President Clinton in the section Annex A: Structure and Organization under the description of Information Sharing and Analysis Center (ISAC), it states, "***Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC****. The center could* ***also gather, analyze and disseminate information from the NIPC for further distribution to the private sector****. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government*."

- Per the FEMA website, "*In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters.*"

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: Carrie Dixon, Xcel Energy, Inc. , 6; - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	
Document Name	

Comment

Xcel Energy appreciates the work the CIP-008-6 Standard Drafting team has done in the limited timeframe it was required to operate within. The second draft effectively addressed industry concerns from the first draft while preserving the intent of the Commission's directive. While Xcel Energy is voting Affirmative, there are a few language changes, in addition to the comments above, that would provide additional clarity. Those changes are as follows:

- In Requirements R2.1 the (S) was removed. We believe that this creates a subject-verb agreement issue. If we one were to say "*Test each Cyber Security Incident response plan at least once every 15 calendar months*:" than there is an indication that a Responsible Entity (RE) has more than one plan, many REs will only have one. However, if we were to say "*Test Cyber Security Incident response plan(s) at least once every 15 calendar months*:" it suggests that an RE may have one or more plans.
- The indication that REs need to have more than one plan is initially described in the already enforced parent Requirement of R2 where it states: "*Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include…*" If R2 were to read "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include…" and then state in "*Test Cyber Security Incident response plan(s) at least once every 15 calendar months*:" we would have agreement in the parent requirement an in the sub requirement that a RE can have one or more plans to collectively address each applicable Requirement.
- In R2.2 language is added that states: "…*that attempted to compromise a system identified in the "Applicable Systems" column for the Part*,…". It is not clear to which Requirement Part the *"Applicable Systems" column for the Part"* is referring to. Xcel Energy recommends adding the part number (i.e. Part 2.2) to each occasion where a Requirement Part is referenced with the Requirement Language or removing the references to the Part altogether.
- Generally, Xcel Energy SMEs feel that the changes made to CIP-008-5 in both Drafts 1 and Drafts 2 were done hastily and in a piecemeal way that were hard to follow and interpret. While Xcel Energy understands that this is likely a bi-product of the shortened drafting period created by the Commission, we also believe that NERC Standards need to be written in a concise and direct way so that no ambiguities exist nor interpretations needs to be made by Responsible Entities. When an existing Standard is open for modification or a new Standard is being

drafted, it is imperative that industry drafts a well written Standard that accomplishes the intent of mitigating the risk and eliminates all possible ambiguities that could lead to misinterpretations and possible compliance violations.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2, Group Name ISO/RTO Standards Review Committee

Answer	
Document Name	

Comment

In requirement R2, part 2.2, please consider changing the following text:

“Cyber Security Incident that *attempted* to compromise a system identified in the “Applicable Systems” column for the Part”

To: “Cyber Security Incident that *was only an attempt* to compromise a system identified in the “Applicable Systems” column for the Part “

In requirement R2, part 2.3, please consider changing the following text:

“Cyber Security Incidents that *attempted* to compromise a system identified in the “Applicable Systems” column for this Part. “

To: “Cyber Security Incidents that *were only an attempt* to compromise a system identified in the “Applicable Systems” column for this Part. “

Likes 0	
Dislikes 0	

Response

Sandra Shaffer - Berkshire Hathaway - PacifiCorp - 6

Answer	
Document Name	

Comment

: We support the extraordinary effort by the SDT, particularly with the extraordinarily short deadline from FERC. In FERC Order 848, ¶ 67, FERC stated, “the development of a Reliability Standard provides the Commission with an opportunity to review and ultimately approve a new or modified Reliability Standard, ensuring that the desired goals of the directive are met.” Moreover, the Reliability Standards development process allows for the collaboration of industry experts in developing a draft standard and also gives interested entities broader opportunity to participate and comment on any proposal that is developed.

The FERC directed timeframe and NERC's scheduling are NOT achieving FERC's statement that the development process allows collaboration and opportunity to participate and comment. The rushed timeframes, **especially a 15-day comment period that includes a holiday week is not acceptable**. Entities did not have time to engage experts within there organizations or trade associations. This comment period also overlaps with the comment period for multiple proposed massive changes to multiple CIP standards and definitions to address virtualization and other.

Won't agree to **define** "attempts" parameters.

There are no questions in the comment form for Part 2.2 or 2.3. We do not support the proposed changes to the Requirements language. *See comments in question #2*.

There are no questions to provide comments on Requirement 4 or its Parts. We do not support these as proposed. With our recommendations in questions 1 and 2, **R4 only needs to refer to Reportable Cyber Security Incidents**. It does not need to include "a Cyber Security Indicent that was only an attempt to compromise a system identified in the "Applicable Systems" column. This phrase should be deleted.

Part 4.1: Include the following attributes, at a minimum, to the extent known: (4.1.1.-4.1.3 as proposed)

Part 4.2: Provide initial notification within the following timelines after determination of a Reportable Cyber Security Incident per Part 1.2: One hour after determination for compromises or disruptions. By the end of the next calendar day after determination for attempts.

Part 4.3: ok as proposed.

There are no questions in the comment form for the proposed Implementation Guidance or Technical Rationale and there has been insufficient time to review the amount of material presented in those two documents to provide comment with this draft. However, there are two initial comments.

Per the FERC Order 848, footnote 19 on page 13, the reference to reliability tasks says, the reliability tasks are referenced in the NERC Functional Model, not the BROS for CIP-002 as noted in the Implementation Guidance.

The Technical Rationale still refers to Reportable Attempted Cyber Security Incidents, *which is no longer a proposed defined term*, on page 4 in the first paragraph under Notification Timing.

All three Parts should follow the pattern in action-oriented Parts and start with verbs.

Dual reporting still not a resolved matter: It is not a consistent, and annonimity is not inplace for both required reporting entities. This needs to be addressed before going forward with this dual reporting requirement.

Refer to :

BROS for CIP-002

FERC Order 848, footnote 19 on page 13

FERC Order 848, ¶ 67

Freedom of Onformation Act

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417

*NCCIC – three things: Functional Impact, Level of Intrusion, Attack Vector…Compared to the NERC implementation guiadance – there is no contunity!

Likes 0	
Dislikes 0	

Response

Kevin Salsbury - Berkshire Hathaway - NV Energy - 5

Answer	
Document Name	

Comment

NV Energy would once again like to commend the SDT on the work done for this Standard, given the time constraints required for completing this project.

NV Energy would like to identify the following gaps between the comment questions and the CIP-008-6 Draft 2:

- There are no questions associated with this Draft's revisions to Requirement R2, Parts 2.2 and 2.3
- There are no questions associated with this Draft's revisions to Requirement R4
- There are no questions associated with this Draft's supplementary documentation: Implementation Guidance and Technical Rationale.

NV Energy believes there should be avenue for providing comments for all revisions within the Requirement language, and supplementary documentation.

NV Energy would also like to provide commentary on the poorly chosen timeframe for this commenting and balloting period for CIP-008-6. With the pool and commenting period opening on the Friday prior to the week of a federal two-day holiday, made it very difficult to engage our company experts, and trade associations, to review the revisions within this Draft. In addition to the holiday, the commenting and ballot period for CIP-008-6 is occurring concurrent to the commenting for the revisions to the CIP Standards due to Virtualization inclusion, which included extensive changes to CIP Glossary Terms and five (5) CIP Standards.

NV Energy understands that there is a strict timeline imposed for the approval of CIP-008-6, but this timeline should not impose on the industry's ability to provide fully vetted commentary and ballot position.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

EEI believes that the SDT and NERC deserve recognition for exceptional work addressing FERC directives under a very aggressive timeline while still effectively considering and addressing Industry concerns.

One additional suggested minor change would be the following to Part 2.2:

"Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, ***and/or*** Cyber Security Incident that attempted to compromise a system ***as*** identified in the "Applicable Systems" columns ***under Requirement R1***, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise."

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	
Document Name	

Comment

Exelon would encourage the Standards Drafting Team (SDT) to assist Responsible Entities by providing a clear description in the Implementation Guidance of the scope of equipment in scope. Additional discussion around how PCA's are not included, as an example, will help entities properly scope their reporting program to the standard. We also believe it would be a good clarifying change to the definition of Reportable Cyber Security Incident to explicitly note that PCAs are not included in scope. We do not believe this is a substantive change to the standard, but reflects what is currently drafted. Additional explanation would be beneficial in clearly articulating scope of the standard.

Likes 0	
Dislikes 0	
Response	
Davis Jelusich - Public Utility District No. 1 of Chelan County - 6, Group Name Public Utility District No. 1 of Chelan County	
Answer	
Document Name	
Comment	
Although FERC requested reports be sent to both E-ISAC and NCCIC, this inefficiency may distract or impair a responsible entity's incident response. These government organizations should share reports instead of placing the burden on each entity.	
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	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	

Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	
Document Name	

Comment
As per our response to Question 1, N&ST believes Protected Cyber Assets (PCAs) should be included with BES Cyber Systems and associated EACMS as applicable systems.

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	
Document Name	

Comment
There are no questions in the comment form for Part 2.2 or 2.3. We do not support the proposed changes to the Requirements language. See comments in question 2. There are no questions to provide comments on Requirement 4 or its Parts. We do not support these as proposed. With our recommendations in questions 1 and 2, R4 only needs to refer to Reportable Cyber Security Incidents. It does not need to include “a Cyber Security Incident that was only an attempt to compromise a system identified in the “Applicable Systems” column.” This phrase could be deleted. All three Parts should follow the pattern in action-oriented Parts and start with verbs. Part 4.1: Include the following attributes, at a minimum, to the extent known: (4.1.1.-4.1.3 as proposed) Part 4.2: Provide initial notification within the following timelines after determination of a Reportable Cyber Security Incident per Part 1.2: One hour after determination for compromises or disruptions. By the end of the next calendar day after determination for attempts.

Part 4.3: ok as proposed.

There are no questions in the comment form for the proposed Implementation Guidance or Technical Rationale and there has been insufficient time to review the amount of material presented in those two documents to provide comment with this draft. However, there are two initial comments.

The Implementation Guidance on page 11 below Figure 5 still references the BES Reliability Operating Services (BROS) with respect to reliability tasks. In the FERC order, the reference to reliability tasks is in footnote 19 on page 13. The footnote says the reliability tasks are referenced in the NERC Functional Model, not the BROS. See also the Commission Determination in FERC Order 791 paragraph 156, "While some commenters suggest that the phrase "reliability tasks" is best understood as referring to the bulk electric system reliability operating services listed in the Guidelines and Technical Basis section of CIP-002-5, we believe that the NERC Functional Model is the basis for the phrase "reliability task" while the Guidelines and Technical Basis section provides clarity on how the term applies to the CIP version 5 Standards."

The Technical Rationale on page 4 in the first paragraph under Notification Timing still refers to Reportable Attempted Cyber Security Incidents, which is no longer a proposed defined term. The capitalization should be removed.

We support the extraordinary effort by the SDT, particularly with the extraordinarily short deadline from FERC. In the Order, FERC stated in paragraph 67: "the development of a Reliability Standard provides the Commission with an opportunity to review and ultimately approve a new or modified Reliability Standard, ensuring that the desired goals of the directive are met. Moreover, the Reliability Standards development process allows for the collaboration of industry experts in developing a draft standard and also gives interested entities broader opportunity to participate and comment on any proposal that is developed.

The FERC directed timeframe and NERC's scheduling are NOT achieving FERC's statement that the development process allows collaboration and opportunity to participate and comment. The rushed timeframes, especially a 15-day comment period that includes a holiday week is not acceptable. Entities did not have time to engage experts within their organizations or trade associations. This comment period also overlaps with the comment period for proposed massive changes to multiple CIP standards and definitions to address virtualization and other.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 6

Answer	
Document Name	

Comment

LES supports the idea of timely information sharing with E-ISAC and in turn E-ISAC providing pertinent information to the industry. While the concern at hand is that not enough information is being provided to E-ISAC, the opposite also appears to be true in that many no-impact and isolated matters are sent out to the industry through E-ISAC alerts. Theses matter of no-impact (and no potential impact) do not appear to serve the industry well and instead only lead to alert fatigue. The drafting team may have an opportunity with their work on this issue to emphasize to E-ISAC that there is an opportunity for improvement in their analysis and their ultimate dissemination of entity provided information. The overall goal of this standard, in coordination with the work of the E-ISAC, should be to ensure the timely and full submission of pertinent data to E-ISAC and then providing the needed information to the industry through E-ISAC alerts.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	
Document Name	

Comment

We generally agree with the approach the SDT has taken. However, PCAs should be included in the Applicable Systems column for requirements and in the definitions for Cyber Security Incident and Reportable Cyber Security Incidents due to their association with BES Cyber Systems and potential for revealing malicious activity directed at the BPS.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	
Document Name	

Comment

No additional comments.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2

Answer	
Document Name	
Comment	

We agree with the comments provided by the IRC Standards Review Committee. While we are voting for the standard, we believe the following changes would improve and simplify the standard, while making it more adaptable to changing conditions:

- Regarding R2, we believe an implementation of the plan, to include notification of an incident or an attempt, should constitute a test of the plan. The measure for R2 should state this.
- R3 is redundant. The entity is responsible for having a plan in R1. They either have an appropriate plan or they don't. R3 adds an unnecessary obligation to have documentation to prove you have documentation.
- It is our understanding that some entities want additional structure on what gets reported. We believe a requirement on notification is sufficient and believe it should be up to the E-ISAC to work with the industry over time to define the information it needs when an incident gets reported. The structure of the report should not be hard-coded in the standard or an attachment.

Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	
Document Name	
Comment	

Comments: Duplicate effort would be needed to notify multiple agencies.

Likes 0	
Dislikes 0	
Response	
Michael Buyce - City Utilities of Springfield, Missouri - 1	
Answer	
Document Name	
Comment	

Referring to the "Applicable Systems" column in the "Requirements" column may be redundant. A suggestion for the language in the Part 2.2 is: "Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber

Security Incident that was an attempt to compromise (as defined in Part 1.2.1) one or more applicable systems, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise”

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	
Document Name	

Comment

We do not find language reflecting provisions for CIP Exceptional Circumstances within CIP-008, so there is no safe haven in the event of “*A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure****; a Cyber Security Incident requiring emergency assistance****; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.” It seems that CIP-008 should have language related to CEC as well.*

We understand from the CIP-008 revisions webinar that the SDT declined to include this as part of this project. We strongly encourage the SDT to incorporate language to support CEC relative to CIP-008 as this standard will likely be filed with FERC prior to the completion of the Ballot Process for CEC under Project 2016-02.

Likes 0	
Dislikes 0	

Response

William Sanders - Lower Colorado River Authority - 1

Answer	
Document Name	

Comment

As responsible entities will be required to report more detailed cybersecurity incident information with both E ISAC and DHS once CIP-008-6 becomes effective, both organizations (E ISAC and DHS) should provide a secure electronic method for reporting incidents using existing portals or other means.

Likes 0	
Dislikes 0	

Response
Teresa Cantwell - Lower Colorado River Authority - 5
Answer	
Document Name	
Comment
As responsible entities will be required to report more detailed cybersecurity incident information with both E ISAC and DHS once CIP-008-6 becomes effective, both organizations (E ISAC and DHS) should provide a secure electronic method for reporting incidents using existing portals or other means.
Likes 0	
Dislikes 0	
Response
Barry Lawson - National Rural Electric Cooperative Association - 4
Answer	
Document Name	
Comment
NRECA appreciates the efforts of the SDT on this project and also thanks the SDT for the modifcations made in response to our comments.
Likes 0	
Dislikes 0	
Response
Andrea Barclay - Georgia System Operations Corporation - 4
Answer	
Document Name	
Comment
We appreciate the efforts of the SDT on this project and also thanks the SDT for the modifcations made in response to our comments.
Likes 0	
Dislikes 0	
Response

Patricia Boody - Lakeland Electric - 3	
Answer	
Document Name	
Comment	

We do not find language reflecting provisions for CIP Exceptional Circumstances within CIP-008, so there is no safe haven in the event of "*A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure****; a Cyber Security Incident requiring emergency assistance****; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability." It seems that CIP-008 should have language related to CEC as well.*

We understand from the CIIP-008 revisions webinar that the SDT declined to include this as part of this project. We strongly encourage the SDT to incorporate language to support CEC relative to CIP-008 as this standard will likely be filed with FERC prior to the completion of the Ballot Process for CEC under Project 2016-02.

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	
Document Name	
Comment	

Change the sentence in CIP 008 R2 Part 2.2: The sentence currently reads "Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, Reportable Attempted Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part, or performing an exercise of a Reportable Cyber Security Incident." Change to "Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident and Reportable Attempted Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part, or performing an exercise of a Reportable Cyber Security Incident."

Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	

Recommend the SDT consider including "Cyber Security Incident that attempted to compromise a system identified in the Applicable Systems column" to Part 2.1 in one of the scenarios for testing each Cyber Security Incident response plan. A test of the plan should address all required Parts from R1 no matter the scenario, whether Reportable or attempted Cyber Security Incidents, and exercise SMEs ability to discern the difference.

Recommend the SDT consider adding Physical Security Perimeter (PSP) or associated 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).

Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	
Comment	

Seattle City Light supports these changes in principle, but casts a NO ballot for two reasons. One, to encourage another effort at creating a single report (see discussion in Question 9, above). And two, to encourage additional implementation guidance to add clarity as to how each action reflects a reliability objective and to discuss alternatives to the single approaches, in most case, that are presented.

City Light has two additional questions about proposed CIP-008-6. One, there is a necessity to notify the local Reliability Coordinator if a BROS capability has been compromised. Clarification would be helpful of how this process is envisioned to work in conjunction with CIP-008-6 notificaitons and EOP-004 notifications. Two, what is done with notification information entities make to E-ISAC and DHS? Additional documentation is desired about the subsequent sharing, processing, and storage of notification data, so that appropriate Federal designations (CEII or similar) may be made as appropriate.

Finally, Seattle City Light also would like to propose that the SDT consider the possibility that, if an entity participates in the voluntary E-ISAC CRISP program, such participation would automatically satisfy all reporting requirements of CIP-008. CRISP is a public-private cyber threat and data sharing platform coordinated by E-ISAC and DOE. Participants voluntarily share IT system traffic in near-real time by installing an information-sharing device at the border of the IT systems, just outside the firewall.

Such an approach to CIP-008 reporting has a double benefit. It encourages greater participation in CRISP, which in turn increases the value of the program. It also provides an increased flow of raw cyber security data from industry. This would be an opportunity for FERC and NERC to offer entities a carrot in place of the usual reliability Standard stick.

Other similar IT data sharing platforms, such as that being developed by DHS, might be afforded similar standing as regards CIP-008 reporting.

Additional information about CRISP is available here: https://www.energy.gov/sites/prod/files/2018/09/f55/CRISP%20Fact%20Sheet.pdf	
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 MRO's NERC Standards Review Forum (NSRF) comments.	
Likes 0	
Dislikes 0	
Response	
Dana Klem - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The NSRF recommends that the SDT add language around the Requirement to report “attempt to compromise” recognizing Entities are allowed flexibility by detrmining their criteria based on each entity’s architecture and that a “singular criteria” (one size fit all) will not be effective for applicable entities. We further recommend that this guidance be within the Implementation Plan or Guidance documents that the SDT has developed.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	
Document Name	
Comment	

CIP-008-5 applicability addresses high and medium impact BCS and their associated EACMS, however, it is also recommended to address PCAs as part of the scope. As the new draft definition of a Cyber Security Incident and Reportable Cyber Security Incident reference "the attempted compromised or the compromise of an Electronic Security Perimeter", how can PCAs not be included or are they implied? In the CIP-005-5 Table R1 – Electronic Security Perimeter the Applicable Systems column within the CIP-005-5 Standard PCAs associated with High and Medium Impact BES Cyber Systems are included and make up an Electronic Security Perimeter (ESP). Not listing or including PCAs in the applicability section of CIP-008-6 is inconsistent with the current CIP-007-6 and CIP-010-2 Standards as they ensure the same level of preventative security controls and baselines are applied to PCAs that make up the ESP as a whole.

Part 2.1 should be modified to permit exercise of the plan using any Cyber Security Incident. Restricting the exercise to only Reportable Cyber Security Incidents restricts the exercise to only a subset of an entity's incident response plan. Part 2.2 should be simplified to require use of the incident response plan when responding to any Cyber Security Incident.

Likes 0	
Dislikes 0	

Response

Vivian Vo - APS - Arizona Public Service Co. - 3

Answer	
Document Name	

Comment

AZPS respectfully recommends removal of the word "only" from the following:

- Part 1.2.2
- Measures for Part 2.3
- R4

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

In requirement R2, part 2.2, please consider changing the following text:

"Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for the Part"

To

“Cyber Security Incident that was only an attempt to compromise a system identified in the “Applicable Systems” column for the Part “

In requirement R2, part 2.3, please consider changing the following text:

“Cyber Security Incidents that attempted to compromise a system identified in the “Applicable Systems” column for this Part. “

To

“Cyber Security Incidents that were only an attempt to compromise a system identified in the “Applicable Systems” column for this Part. “

Likes 0	
Dislikes 0	

Response

Richard Jackson - U.S. Bureau of Reclamation - 1

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, Reclamation recommends the SDT 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).

After the change to Requirement R1 Part 1.1 measure is incorporated, Reclamation recommends the SDT 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. - 3, Group Name AECI

Answer	
Document Name	

Comment

AECI supports comments provided by NRECA

Likes 0	
Dislikes 0	

Response

Kevin Conway - Public Utility District No. 1 of Pend Oreille County - 1

Answer	
Document Name	

Comment

We agree with the direction of the Drafting team, but are concerned that there is not enough protection from subjective enforcement by auditors and enforcement staff. The danger is most apparent when the entity is trying to meet the spirit of the standard but held to a best practices threshold.

Likes 0	
Dislikes 0	

Response

Russell Martin II - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
No comment from SRP	
Likes 0	
Dislikes 0	
Response	
Leanna Lamatrice - AEP - 3	
Answer	
Document Name	
Comment	
AEP recommends striking the word “only” from the sentences which include, “….Cyber Security Incident was only an attempt to compromise a system identified in the “Applicable Systems” column for this Part.” In requirement R4 and part 4.2. This is to be consistent with requirement parts 2.2 and 2.3 and the definition of Cyber Security Incidnet.	
Likes 0	
Dislikes 0	
Response	

Comments received from Jack Cashin, APPA

1. The Standard Drafting Team (SDT) has an updated approach regarding new and modified terms. The SDT is no longer proposing a new definition for reportable attempted cyber security incidents. The defining concepts describing this event have been incorporated in proposed modifications to Requirement R1, Part 1.2.1 and Part 1.2.2. The Responsible Entity will be required to establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems. The SDT is proposing modifications to Cyber Security Incident as well as Reportable Cyber Security Incident. For Reportable Cyber Security Incident, the SDT has determined it is prudent to include BES Cyber Systems (BCS) because of their criticality in relation to ESPs. By including BCS in the Reportable Cyber Security Incident definition, it shows that Protected Cyber Assets (PCA) are not in scope for the proposed modification. Do you agree with the proposed modified definitions of, Cyber Security Incident and Reportable Cyber Security Incident? Please provide comments and alternate language, if possible.

Yes
x No

Comments:
APPA believes that additional guidance on the language on alternative approaches -- “establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable system,” is needed.
Public power concurs that PCAs should not be included in the proposed modification to the standard.

2. The SDT has added language in Requirement R1 Part 1.2. for the Responsible Entity to establish and document criteria to evaluate and define attempts in their Cyber Security Incident response plan(s). Do you agree with this approach to allow the entity to define attempts for their unique situation?

X Yes
No

Comments: APPA supports the intent of the proposed changes but, as stated in the answer to question 1, believe the Standard would benefit from guidance on alternative approaches addressing the language,“establish criteria to evaluate and define attempts and determine if a Cyber Security Incident is an attempt to compromise one or more applicable systems.”
We are concerned that without established guidance, complying entities and compliance and enforcement staff do not have sufficient guidance to come to a common understanding of the draft standard language. Complying public power entities believe that a conservative reporting criteria will present significant costs to administer without corresponding measurable reliability benefits. The costs required for the follow-up requirements in R4 are significant.

3. Do the changes clarify that the Responsible Entity must have a process to determine what is an attempt to compromise and provide notification as stated in Requirement R1 Part 1.2 and Requirement R4 Part 4.2? Please explain and provide comments.

X Yes
No

Comments: APPA believes that the proposed changes reflect that an Entity must have a process in place to identify compromise attempts and provide notification. Public power is concerned that specifying a specific number of days for reporting actual, and attempted Cyber Security Incidents to agencies could lead to resource challenges. Public power recommends that the SDT consider a time frame that provides an update within 24 hours of actual determination of the criteria established in R4.1. Physically getting a team to remote substations to determine the attack vector could take time, and the difficulty will increase depending on how wide-spread the event turns out to be.

4. 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? Please provide comments and an alternate approach to addressing the directive, if possible.

x Yes
No

Comments: Because there is another SDT evaluating the term EACMS, APPA would appreciate further guidance from the CIP-008 SDT on whether just the proposed EACS or both the proposed EACS and EAMS would be included in the revised CIP-008 requirements.

5. Do you agree with reporting timeframes included Requirement R4 Part 4.2 and Part 4.3 which include an increase in reporting timeframe from 5 to 7 calendar days in Part 4.3? Please explain and provide comments.

Yes
X No

Comments: APPA appreciates that the SDT has provided additional time for updates to the original notification; however, we are not convinced that the timeframe is appropriate for all situations. The requirement of tracking the periodic updates will add additional administrative burden for utilities and may not add commensurate reliability benefits.

6. Do you agree with the SDT's decision to give the responsible entity the flexibility to determine notification methods in their process? Please explain and provide comments.

Yes
No

Comments: It is not clear what the SDT means with the language, "flexibility to determine notification methods in their process." Is this referring to language in the R 4.2 that was deleted in this version? Otherwise, the "flexibility" is not included. The measures for the new R 4.2 state just a single measure: Examples of evidence may include, but are not limited to, dated documentation of notices to the E-ISAC and NCCIC.

7. Based on feedback the SDT has adjusted the Implementation Plan timeframe from 12 to 18 months. In the Consideration of Comments Summary Report the SDT justified this change. Do you support the rationale to move to an 18-month Implementation Plan? Please explain and provide comments.

X Yes
No

Comments: APPA supports the extended implementation timeframe.

8. Although not balloted, do you agree with the Violation Risk Factors or Violation Severity Levels for Requirement R1 and R4? Please explain and provide comments.

Yes
No

Comments:

9. 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.

Yes
X No

Comments: Public power is concerned that the timeline for reporting creates additional administrative burden and cost. In addition, Entities that have an integrated EOP-004/CIP-008 all hazards approach to incident management will have to expend significant resources to comply with these changes. There is no evidence that reliability and security benefits will be commensurate with the increased costs.

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

Comments received from Brenda Hampton, Luminant Mining Company LLC

Question 1
Luminant agrees with the updated approach; however, the language in 1.2.2 might be improved. Luminant suggests simplifying by combining the bullets to read: "Determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident or an attempt to compromise one or more systems identified in the “Applicable Systems” column for this Part; and"

Question 6
Luminant agrees with providing flexibility to the entity; however, we continue to disagree with the determination that reporting to a single agency as an intermediary to the other agency is outside the scope of the SAR. We also suggest NERC pursue an update to OE-417 to add a checkbox to include the DHS organization (in this case NCCIC). We believe every effort should be made to consolidate reporting to a single entity.

Question 10
Although we believe that it is in industry's best interests to come up with criteria for evaluating "attempts to compromise", we are absolutely opposed to the Implementation Plan as it currently exists. The suggested criteria would leave entities with a ridiculously broad criteria for reporting. We suggest a robust process may be required to come up with better criteria for this category and may need some trial period before finalizing any IP.