NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-008-6

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting: Consideration of Comments

November 2018

RELIABILITY | ACCOUNTABILITY

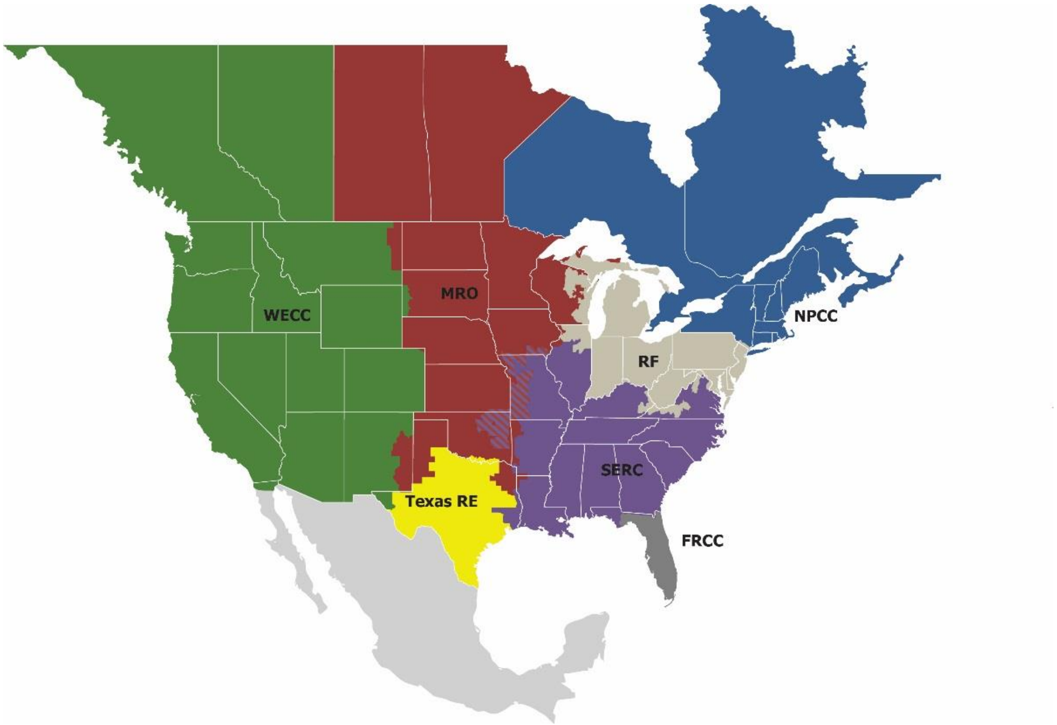
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The vision for the Electric Reliability Organization (ERO) Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the seven regional entities (REs), is a highly reliable and secure North American Bulk-Power System (BPS). Our mission is to ensure the effective and efficient reduction of risks to the reliability and security of the grid.

The North American BPS is divided into seven RE boundaries, as shown below in the map and corresponding table. The downward diagonal, multicolored area denotes overlap because some Load-Serving Entities participate in one region while associated Transmission Owners/Operators participate in another.



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Background

The Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting standards drafting team thanks all commenters who submitted comments on the draft CIP-008-6 standard. This standard was posted for a 20-day public comment period, ending Monday, October 22, 2018. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 86 sets of responses, including comments from approximately 176 different people from approximately 116 companies, representing the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the NERC standards developer, Alison Oswald, at 404-446-9668 or at alison.oswald@nerc.net.

CIP-008-6 Consideration of Comments – Summary Responses

Purpose

The Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting standards drafting team (SDT) appreciates industry's comments on the CIP-008-6 standard. The SDT reviewed all comments carefully and made changes to the standard accordingly. The following pages are a summary of the comments received and the SDT's corresponding responses. If a specific comment was not addressed in the summary of comments, please contact the NERC standards developer.

Definitions

Several commenters asked for clarity in the definitions for attempts to compromise, how BES Cyber Assets (BCAs) are included, and the potential for having only one definition.

The SDT made changes to the requirements to clarify that the Responsible Entity determines attempt to compromise through their processes for reporting. Verbiage has been added to CIP-008 R4, Part 4.2 that links the process to determine reportability defined in CIP-008 R1, Part 1.2 to the obligation to report after the determination is made by the Responsible Entity.

The SDT addressed BCAs by adding BCS to the Reportable Cyber Security Incident definition. The team asserts that the modification aligns with the intention of FERC Order 848 Paragraph 52 that describes BES Cyber Systems within the ESP.

The SDT also reviewed the comments that addressed consolidating the definitions into one definition. The team made the decision to remove the proposed Reportable Attempted Cyber Security Incident definition. Instead, CIP-008 R4, Part 4.2 has been updated to include conditions for reporting Cyber Security Incidents that only attempt to compromise a system identified in the "Applicable Systems" column for this part. The modification does not impact the definitions of Cyber Security Incidents and Reportable Cyber Security Incidents that exist in both CIP-008 and CIP-003, and eliminates the need for a standalone definition for Reportable Attempted Cyber Security Incidents.

Attachment 1

Many commenters expressed concern with requiring reporting to occur in the format of Attachment 1.

Based on comments received and consultation with representatives from the Electricity Information and Analysis Center (E-ISAC) and the National Cybersecurity Communications Integration Center (NCCIC), which is the successor organization to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the standard has been updated such that Attachment 1, and the supporting instructions called Attachment 2 have been removed from the standard and are no longer required. The form and instructions have been moved to draft Implementation Guidance as an option for Responsible Entities to use at their discretion.

Many commenters expressed concern with the methods of submitting the three required attributes being prescriptive and disagree with updates having to be submitted in only Attachment 1 form.

The SDT determined it was not necessary to define the method for notification, and the initial proposed Requirement R4, Part 4.2 has been removed. Attachment 1 is no longer required, and has been moved into the draft Implementation Guidance.

Some commenters mentioned that the new form should fit with other forms and existing reporting requirements to avoid duplication (utilize EOP-004-4 and/or Department of Energy's OE-417)

The SDT has removed the proposed requirement for utilizing the proposed Attachment 1. However, the SDT determined not to modify existing reporting forms, such as OE-417, because Order No. 848 noted that this form did not request information that FERC directed the SDT to require in CIP-008. Nonetheless the SDT notes that entities may consider synchronizing their reporting processes as long as all information that is required to be reported is submitted to appropriate agencies.

Some commenters would like to leverage reporting to a single agency as an intermediary to the other agency.
The SDT thanks you for your comment, however the SDT asserts that the proposed reliability standard is responsive to FERC Order 848 and that this is outside of the scope of the SAR.

Information Protection

One initial point of clarification: ICS-CERT functions are now handled by the Department of Homeland Security (DHS) National Cybersecurity and Communication Integration Center (NCCIC) and incident reports will be submitted through existing NCCIC incident reporting mechanism rather than anything specific to ICS-CERT. Any future references will be to NCCIC, which is ICS-CERT's successor organization.

Many commenters expressed concern over information protection once information is submitted to E-ISAC and NCCIC.
During the meeting the SDT submitted these concerns to both the E-ISAC and NCCIC. Both organizations assured the SDT that they have multiple ways to secure information that is submitted. Options include:

- Utilizing a secure/encrypted portal; or
- Encrypted e-mail (via Pretty Good Privacy – PGP)

Please note the following answers are directly from DHS.
Many commenters expressed concern if DHS will make the information reported public.
DHS will not attribute any information back to an entity but may incorporate the non-attributable and anonymized information into publicly available products to enable stronger cybersecurity protections and response activities for similarly situated entities. Such use or incorporation will only be done without attribution to the original entity and with the removal of any contextual information that could enable an entity's identification, unless the entity expressly agrees otherwise in writing.

Many commenters expressed concern about what confidentiality provisions will be in place for information submitted to DHS.
DHS will not attribute any information back to an entity and will use cover names for the entity within the NCCIC to protect the entity's identity. Information submitted through email can be done so with the DHS PGP key to keep information confidential. In addition, the web-based portal has security in place to protect information submitted through that option.

Many commenters wanted assurances that phone conversations with DHS are confidential.
Submissions by phone are added to the incident management system as tickets and are entitled to the same protections as submissions provided through email or web form.

Many commenters expressed concern over where reported data will be stored at DHS.
Data will be handled and stored with other sensitive incident reporting data the NCCIC receives and triages from various public and private sector entities.

Many commenters asked who will be liable for a data breach at NCCIC.
DHS has no comment regarding this issue.

Many commenters expressed concern that the reports submitted to DHS will be subject to Freedom of Information Act (FOIA) requests.

DHS has successfully exempted similar information from FOIA in the past under various FOIA exemptions defined at 5 U.S.C. § 552(b), to include Exemption (b)(3) as specifically exempt from disclosure by statute, Exemption (b)(4) as trade secrets and commercial or financial information that is privileged or confidential, and Exemption (b)(7)(A)-(F) as records or information compiled for law enforcement purposes. To the extent incident reports contain cyber threat indicators and defensive measures that meet the definition of cyber threat indicator or defensive measure as defined in the Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1501-1510 ("CISA"), and that is provided in accordance with CISA's requirements, such information will be protected as provided by CISA (including protection from release under FOIA). See the Non-Federal Entity CISA Sharing Guidance published by the Department of Homeland Security and the Department of Justice, available at https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

Many commenters inquired if entities will receive confirmation receipt or other methods to ensure DHS received information.

DHS will provide entities with a ticket number upon receipt of information.

Notification Approach

Many commenters suggested increasing the initial notification timeframe for attempts to compromise (which was defined in the first proposed draft as a Reportable Attempted Cyber Security Incident) from the next calendar day to the next business day.

The SDT asserts the end of the next calendar day is sufficient time for notification. The preliminary notification is not triggered until a Responsible Entity has made a determination on classification of reportability and does not require all of the attributes to be identified if undetermined at the time of notification. The determination defines the start time for reporting. Business day is a difficult term to define, particularly in 24x7 business environments. However, the SDT asserts that the end of a calendar day is understood to be 11:59pm local time.

Some commenters suggested increasing the initial notification timeframe for Reportable Cyber Security Incident from 1 hour to 2 hours.

FERC Order No. 848 instructs the SDT to consider risk when developing timeframes. The SDT asserts that the 1 hour timeline is in alignment with previous versions of CIP-008, other FERC orders, and severity of the incident. This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable. It does require preliminary notification, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report. The SDT also asserts that means exist to provide simultaneous notification. The time required to notify additional entities does not begin until the entity has made a determination that aligns with a reportable classification.

Many commenters suggested increasing the timeframe for updates to the three required attributes to within 7 days instead of 5 days.

The SDT has adopted this recommendation.

Many commenters expressed confusion that initial notification and updates are not required until an incident is "determined" by an entity to be reportable or reportable attempted.

The SDT has added clarifying language in Requirement R4, Part 4.2 that refers to Requirement R1, Part 1.2, where Responsible Entities define their process(es) for determination of reportability.

Attempts

Several commenters expressed concern about the determination of "attempts" and requested the SDT either define "attempts" or provide clear examples within Implementation Guidance to aid the industry.

The SDT asserts that it is to the industry's benefit that CIP-008 leaves it up to each Responsible Entity to document a process to determine what constitutes an "attempt". The SDT further asserts that no two Responsible Entities are alike and the determination of "attempts" is contextual and dependent on what is normal within each unique organization. To define "attempt" could create an overly prescriptive and less risk-based approach and may have the unintended consequence of undue administrative burden or removal of needed discretion and professional judgment from subject matter experts. The SDT has developed proposed Implementation Guidance inclusive of several examples in an effort to address this issue.

Some commenters suggested monthly reporting for minimal risk attempts to the ERO and questioned the value of proposed reporting timeframes.

Thank you for your comment. The SDT asserts that the reporting timeline for attempts to compromise is in alignment with FERC Order No. 848 and is in the spirit of timely reporting for information sharing.

PSPs

Commenters expressed confusion on how the standard relates to Physical Security Perimeters (PSP) and in some instances requested the removal of PSP from the Cyber Security Incident definition.

Regarding PSPs, the currently enforceable definition of Cyber Security Incident includes malicious acts or suspicious events that compromise, or attempt to compromise, PSPs. The currently-enforceable Reportable Cyber Security Incident definition includes Cyber Security Incidents that have compromised or disrupted one or more reliability tasks of a functional entity. As such, compromises or attempts to compromise PSPs could be reportable under the currently enforceable standard and definition. The SDT understands the concern but determined not to lessen the reporting obligation from that of the currently enforceable standard. In addition, the SDT reviewed the directives from FERC Order No. 706 that directed NERC to take into account in CIP-008 a breach that may occur through cyber or physical means. As a result, the SDT will not remove PSP from Cyber Security Incident. As an example, this issue is also addressed in CIP-006-6, Requirement R1, Part 1.5, among others, where Responsible Entities must issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.

Some commenters wanted to understand the omission of Physical Access Control Systems in the Applicable Systems column of the standard.

The SDT asserts the modifications proposed are in response to FERC Order No. 848.

EACMS

Multiple commenters were concerned that the inclusion of the five functions modified the definition of Electronic Access or Monitoring Control Systems (EAMCS) and either narrowed or broadened the scope of that definition.

The SDT considered comments regarding the inclusion of the five EACMS functions within the proposed revised definition for Reportable Cyber Security Incidents and what had been a new proposed definition for Reportable Attempted Cyber Security Incidents in the first draft. The industry was divided on this subject in that some entities view the inclusion of these functions as an attempt to modify or expand the scope of the existing EACMS definition and want it stricken, while others view the inclusion as a limiting factor and prefer to retain the language in the definitions. *The SDT concluded that neither the inclusion nor exclusion affects the current definition of EACMS.*

The SDT asserts that the inclusion of these five functions within this proposed definition is unnecessary and not appropriate at this time. The SDT discussed at length both sides of the issue and decided to remove the five functions for the following reasons:

1. The team has adjusted the definition of Reportable Cyber Security Incident and the Applicable Systems column and requirement language for attempts to compromise to align directly with the FERC Order

Paragraph 54 and believes these five functions are the essence of an EACMS by the current definition and to restate them is redundant.

2. The inclusion of these functions may create a new sub-classification EACMS resulting in potential confusion and undue administrative burden for Responsible Entities to establish and implement new processes to reclassify. This may unnecessarily complicate, create confusion, or introduce delay in timely information sharing.
3. Regional inconsistencies with interpretation should be referred to NERC staff for evaluation of and submission through the alignment tool. NERC Project 2016-02 is also in the process of modifications to the NERC Glossary of Terms definitions for Interactive Remote Access, Intermediate Systems, and Electronic Access Control or Monitoring Systems. Additionally, the Project 2018-02 SDT has decided not to modify these terms due to their pervasive use throughout CIP Reliability Standards and the abbreviated timeline for filing of CIP-008-6 as directed in FERC Order No. 848.
4. In addition, while the SDT understands the potential for opposing interpretation, the use of the words "at a minimum" in FERC Order No. 848 Paragraph 54 suggest an intention to limit scope, which the SDT will address within Technical Rationale and Interpretation Guidance.

The SDT reevaluated FERC Order No. 848 and asserts that these five functions align with the directive in Paragraph 54 and are also are consistent with the EACMS definition. By definition, EACMS are, "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) (ESP) or BES Cyber Systems. This includes Intermediate Systems." When analyzing these five functions against this definition, the SDT determined each function is traceable to a component of the EACMS definition. The following list is a mapping of the five EACMS functions from the FERC directive to the current enforceable definition in demonstration of this alignment.

An EACMS associated to a High or Medium impact-rated BES Cyber System (H/M BCS):

(1) performing an **authentication** function, constitutes a Cyber Asset that performs electronic access control of the ESP or BES Cyber Systems;
(2) performing a **monitoring and logging** function constitutes a Cyber Asset that performs electronic access monitoring of the ESP or BES Cyber Systems;
(3) performing an **access control** function constitutes a Cyber Asset that performs electronic access control of the ESP or BES Cyber Systems;
(4) performing an **Interactive Remote Access** function constitutes a Cyber Asset that performs electronic access control of the ESP or BES Cyber Systems; and
(5) performing an **alerting** function constitutes a Cyber Asset that performs electronic access monitoring of the ESP or BES Cyber Systems.

Some commenters asked that the five functions be put in the Applicable Systems column or the requirement language.
The SDT concluded that neither the inclusion nor exclusion affect the current definition of EACMS and chose not to include the five functions in the Applicable Systems column. Please see justification above to support this decision.

Some commenters asked the SDT to modify the EACMS definition.
The SDT evaluated the potential impact and unintended consequences due to its pervasive use throughout the standards and elected not to modify the EACMS definition.

Commenters were concerned that adding EACMS to the Applicable Systems column was pulling in new monitoring or alerting systems and creating a "hall of mirrors."
The SDT is not modifying the existing definition of EACMS. Adding EACMS to the Applicable Systems column does not change which Cyber Assets are classified under the currently-enforceable standard as EACMS.

Commenters suggested EACMS does not need to be in the definition if it is in the Applicable Systems column.
The SDT asserts that the presence of EACMS in the Reportable Cyber Security Incident definition and the Applicable Systems column provides clarity and aligns with FERC Order No. 848 to expand reporting to EACMS.

Implementation Plan

Multiple commenters stated a 12-month implementation phase is not sufficient to accommodate the increased workload associated with increased reporting requirements.
The SDT considered comments related to the amount of time needed for successful implementation of the modifications to CIP-008 (Project 2018-02) and agrees with the need for additional time to make the necessary adjustments. Consequently, the SDT assert that an 18-month implementation timeline is necessary and appropriate for the reasons provided below.

Impact on Small Business Entities
The FERC Directive (Order No. 848) was intended "to result in a measured broadening of the existing reporting requirement" in CIP-008-5, and not create a "wholesale change in cyber incident reporting".1 While this may be true for larger electric utilities, the SDT considered the impact of increased reporting requirements on all NERC-regulated entities and has determined that small-business entities – those with a limited customer base, lower annual revenue/mile of transmission line, and located in rural areas – have fewer resources available to meet increasingly granular requirements, as well as zero-consequence incidents.

Small entities are more susceptible to problems in hiring a number of problems in hiring and retaining cybersecurity staff, including competitive salary, progressive career path, retiring employees, and smaller applicant pools. Lack of trained staff results in increased costs for consulting services for system design and architecture, professional engineering, network design and integration, and technical support. The budget request process to secure consulting services, as well as the resulting recommendations for equipment, requires preparation and justification, and appropriate time is needed.

While the Commission states that entities are already required to perform system security monitoring (CIP-007 Requirement R4), there are certain considerations for smaller entities that may have been overlooked. The difference between logging events (per BES Cyber System or Cyber Asset capability) and reviewing the logged events is significant. Smaller entities may have older equipment (decreased capabilities) and lower-impact BES Cyber Systems (not high-impact which requires review/sampling of logged events) and the new requirements create an increased need for securing additional resources (including trained professionals). For many entities, including not-for-profits, budget approval cycles may exceed 12 months, and the timing of the effective date may make the requirement difficult to achieve for these entities.

New or modified compliance documentation
All NERC-registered entities will bear the burden of developing updated documentation necessary to prove that specific actions, processes, and standards are met, vetted, and approved. The documentation may include updated roles and responsibility matrices, flowcharts, development and implementation of internal controls,

[1] 2018, RTO Insider, *FERC Orders Expanded Cybersecurity Reporting*, July 18, 2018. https://www.rtoinsider.com/ferc-nerc-cybersecurity-96423/

appropriate evidence generation and retention schedules, as well as impact assessment and modification to other existing programs.

In addition, most entities subject to CIP-008 are also required to document processes and report related incidents to NERC, under EOP-004, and to the U.S. Department of Energy (DOE). Recently, DOE updated its primary reporting tool to incorporate questions that are or will be included in the NERC EOP-004 Reliability Standard Event Reporting Form. With the changes to Form OE–417 if a respondent elects to have the form submitted to NERC, the entity does not need to file an EOP–004 Event Reporting Form. Form OE–417 will now collect the same information as EOP–004. By incorporating the same information, and aligning language across these two forms, entities will only be required to submit Form OE–417. This will reduce the reporting burden for the electric power industry.[2]

Unfortunately, the Commission specifically stated that it does not support adopting the DOE Form OE-417 as the primary reporting tool for reporting Cyber Security Incidents because the reporting criteria in its directive are distinguishable and more aligned with a risk management approach than the information requested in the DOE Form OE-417.[3] In addition, the accelerated (6-month) timeframe required to develop modified CIP-008 reporting requirements did not provide the time needed for the SDT to develop a more cohesive reporting approach that would satisfy EOP-004, CIP-008, and DOE in a single report. Therefore, entities are required to develop, document, and implement multiple processes to report similar information to multiple entities. Again, for smaller entities with limited staff resources, this effort may require more than 12 months to successfully achieve.

Enhanced End-User Training

In conjunction with development of new processes and associated documentation, all entities will be required to revise and augment their current training programs, as well as find the time to adequately train all personnel with key roles and responsibilities. This task is further complicated for small entities where the same person(s) may bear the responsibility to identify, report, handle, and respond to the same or similar incidents to multiple entities under multiple timelines – all while preserving the reliability of the BES. Appropriate time is needed to fully evaluate time demands, level of risk, defined roles, and reporting responsibilities and then training, as necessary to provide a sufficient level of assurance.

Responsible Entities would be best served if they are allowed to align the newly developed incident reporting and response training on the entity's current annual training cycle (CIP-004, Requirement R2).

Alignment with existing CIP-008 requirements:

In addition to an established annual training schedule, entities are required under CIP-008 Requirement R2 Part 2.1, to test their Cyber Security Incident response plan(s) on a 15-month schedule. An increased implementation timeframe affords entities the opportunity to embed the plan updates, resulting from the new reporting requirements, into their existing test schedule to achieve maximum benefit.

Network Architecture Modifications

With the additional scrutiny that Cyber Security Incidents involving attempts to compromise will likely require due to the modifications to this standard and associated definitions, entities may consider modifying current network architecture for EACMS and/or Intermediate Systems for Interactive Remote Access which may currently be used for multi-impact BES Cyber Systems (i.e., for High, Medium, and Low impact). Splitting impacts used for each EACMS and Interactive Remote Access solutions may reduce investigation and reporting burden by decreasing the attack surface by taking low-impact BES Cyber Systems out of the equation. These changes will

[2] DEPARTMENT OF ENERGY, U.S. Energy Information Administration, Agency Information Collection Extension With Changes, Federal Register /Vol. 83, No. 7 /Wednesday, January 10, 2018 /Notices.

[3] FERC Order 848 at Paragraph 73.

require deployment of additional resources, modification of many existing security processes, potential implementation of additional security controls, and coordination across large enterprises. Again, due to budgeting cycles, availability of resources, and the need for additional training, the SDT asserts that greater than 12 months is needed to successfully achieve compliance.

A few commenters stated a six-month implementation phase would be sufficient.
The SDT asserts that an 18-month implementation timeline is appropriate (see above). While in certain instances, it may be possible for some entities to implement in a shorter timeframe, the SDT asserts that entities are able to voluntarily share this information at any time, including presently.

VRF/VSLs for Requirement R4

Some commenters noted that the Violation Severity Levels (VSLs) are administrative in nature, could cause unnecessary violations, or should not have a Severe VSL.
The SDT notes that VSLs are considered for penalty sanctions after a violation has been determined based on the language of the requirement. Pursuant to the VSL Guidelines based on the 2008 FERC "VSL Order," Violation Severity Levels must have a severe category as VSLs represent degrees of compliance, not risk to the BES. A severe VSL means that an entity did not meet the performance of the requirement, whereas lesser VSLs show that an entity met some performance of the requirement but not all of the requirement. The SDT agrees that Requirement R4 is administrative in nature so it assigned a “Lower” Violation Risk Factor to reflect the requirement's impact to reliability if violated. However, this consideration does not factor into how VSLs are drafted.

Some commenters suggested the SDT move performance requirements into different VSL categories, such as assigning failure to report what had been previously defined in the first proposed draft as Reportable Attempted Cyber Security Incidents in the Moderate category and assigning a High VSL to failure to notify one of the agencies.
Based on the comments received, the SDT made several changes to the VSLs to incorporate feedback. The SDT revised the Severe VSL to be a failure to take any action under the requirement and added a High VSL to capture when an entity notifies one applicable agency of a Reportable Cyber Security Incident but did not notify the other agency. The SDT also moved failure to report attempts to compromise (formerly defined as Reportable Attempted Cyber Security Incidents) to the Moderate VSL and moved other VSLs regarding Reportable Attempted Cyber Security Incidents to Lower VSL.

Other commenters recommended changes to the VSLs, such as removing Attachment 1 or Reportable Attempted Cyber Security Incidents.
The SDT determined that these comments were more appropriately addressed through considerations to revise the standard or definitions as VSLs are reflections of the requirements and must use language from the standard. In addition to revisions made in response to comments, the SDT revised the VSLs to conform to changes made to the requirements, such as deleting references to Attachment 1, and retracting the definition for Reportable Attempted Cyber Security Incidents and replacing it with requirement language for attempts to compromise, among others.

One commenter suggested revising the VSL to say an entity “did not accomplish initial notification.”
The SDT determined that the "failed to notify" language is consistent with how VSLs are often structured.

Cost Effectiveness

Many commenters expressed concern over the definition of attempts and what would be required to be reported. These commenters noted that this could dramatically increase the workload for these entities and require additional personnel to deal with the reporting requirements and timeframes.
The SDT asserts that CIP-008 is written in a way to allow entities to write a process to define an attempt that is suitable for their organization. The reporting obligations are triggered by a Responsible Entity’s determination of

reportable classification so it is meant to align with the Responsible Entity's timeline and process(es) that define reportability. The SDT asserts that the proposed 18-month implementation plan could work with entities' budget cycles should they determine a need for additional resources.

Other

Several commenters requested the Technical Rationale and Implementation Guidance document be made available at the same time the standard is balloted to provide additional information, intent, examples, and context for a clearer understanding of the requirements.

The SDT plans to post both draft Technical Rationale and draft Implementation Guidance at the time of the second ballot posting.

Several commenters expressed concern about specifying the agency name "ICS-CERT" and "or their successors," and recommended either DHS or the new agency name be used to prevent confusion.

The SDT has replaced references to "ICS-CERT" with the name of its successor entity, the "National Cybersecurity & Communications Integration Center" or "NCCIC" throughout CIP-008. The SDT retained the "or their successors" language to account for any future organization changes.

Several commenters requested clarity regarding required records retention timeframes, including types of documentation needed to demonstrate the number of "cyber ventures or trials" that were not successful reportable attempts or incidents.

As provided in Section C. Compliance, Part 1.2 Evidence Retention of CIP-008, the Responsible Entity is required to keep data or evidence to show compliance for three (3) calendar years, unless its Compliance Enforcement Agency directs a longer period of time as part of an investigation. The SDT asserts that the type of documents to retain are contingent upon each entity's incident plan and associated processes.

Several commenters requested clarity regarding use of "United States" prefacing Responsible Entity in Requirement R4.

The SDT's intent was to exempt Canadian entities from reporting to the U.S. Department of Homeland Security, and Requirement R4 has been modified to address this concern.

One commenter urged that references to "Version 5 CIP Cyber Security Standards" are updated similar to CIP-002-6.

The SDT elected to make minor revisions to the background section. Project 2016-02 will make these conforming changes to the entire suite of CIP standards at a later date.

One commenter suggested including a CIP Exceptional Circumstance (CEC) in CIP-008 with regard to the reporting timeframes.

A general review of CEC is ongoing as part of the scope of Project 2016-02.

Several commenters suggested changing the 60-day requirement for changes to roles/responsibilities, groups/individuals, or technology in Requirement Part 3.2, to 90-days as specified in Part 3.1.

The SDT asserts that modifications of these timeframes are outside of the SDT's scope of work. No changes were made to Requirement R3, and FERC Order No. 848 was silent regarding these Requirement Parts.

Several commenters suggested merging the requirements in Part 1.1 (One or more processes to identify, classify, and respond to Cyber Security Incidents) and Part 1.4 (Incident handling procedures for Cyber Security Incidents) into a new cumulative version of Part 1.1.

The SDT asserts that the only changes proposed to these Parts was to the Applicable Systems column and has elected to make no additional changes to the existing approved language.

Several commenters suggested eliminating use of the term "Responsible Entities" from Table 4, in order to align with language used in the other Tables.

Based on this comment the SDT has eliminated the use in Requirement R4, Part 4.3. The SDT asserts that the term "Responsible Entity" as used in part 4.2 is to clarify that the determination is made by the Responsible Entity in the same manner done in previously approved Table 3, Requirement R3, Part 3.2.

One commenter suggested structuring Requirement R4 similarly to other standards and removing the notifiable entities to a subpart within the Table.

The SDT asserts that Requirement R4, in its totality, covers reporting and listing the agencies in the parent Requirement helps provide clarity with regard to the requirements without the added clutter of repeating the agencies in multiple locations. Any concerns about missing the agency names should be satisfied by language incorporated into the Measures***.***

One commenter suggested adding "Reportable Attempted Cyber Security Incidents" to Requirement R3, Parts 3.1 and 3.2, requiring update of the entity's plan if it is used in response to an attempted incident.

Based on industry concern and lack of measurable statistics on the number of attempts that would be reportable as a result of the proposed modifications, as well as the exclusion of Responsible Entity determined attempts to compromise (formerly defined as Reportable Attempted Cyber Security Incidents in the first proposed draft) satisfying the plan testing requirements, the SDT declines to expand the requirements in Parts 3.1 and 3.2.

A commenter supports the methods of notification, but asks the standard drafting team to include a note in the form to request receiving entities confirm receipt or provide another method of ensuring entities receive such a confirmation.

The SDT asserts that directing E-ISAC or NCCIC to provide such confirmation is not within our purview. The obligation for capturing and documenting required evidence of reporting is on the Responsible Entity. The proposed requirements do not preclude the Responsible Entity from incorporating steps into their process to request confirmation at the time of notification.

One commenter asked whether an actual "Reportable Attempted Cyber Security Incident" would be considered a test of the entity's plan under Requirement Part 2.1.

Thank you for your comment, the SDT intentionally excluded attempts to compromise (formerly defined as Reportable Attempted Cyber Security Incidents in the first proposed draft) from Requirement R2, Part 2.1. Please see Technical Rationale for justification.

Several commenters requested removal of cross-references in Parts 1.2 and 4.2.

The SDT asserts the cross-referencing provides clarity and beneficial reinforcement.

One commenter suggested periodic reporting (monthly or quarterly) should be simplified, such as the IP address and service or port that was blocked, which would still provide the reporting and data necessary to meet the intent of FERC Order No. 848.

The SDT asserts that periodic reporting would not provide the timely information required by the Commission and that automated reporting would not clearly provide the required attributes.

One commenter felt that the concept of "Reportable Attempted Cyber Security Incident" is nebulous and the modifications could result in reporting with little value.

The Reportable Attempted Cyber Security Incident definition has been removed by the Standards Drafting team. Instead, the team leveraged the existing Cyber Security Incident definition, and modified the proposed CIP-008 R4, Part 4.2 language to qualify that attempts to compromise a system identified in the "Applicable Systems", including High Impact BES Cyber Systems and their associated EACMS and Medium Impact BES Cyber Systems and their associated EACMS, are reportable after the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2.

One commenter noted that CIP-008-6 Requirement R1, Part 1.2 requires the Incident Response Plan to include processes to determine whether an incident is reportable, but does not require a documented process for notification, even though the measures for Part 1.2 reference "documented processes for notification."
The SDT addressed this comment by making modifications to the proposed standard language in Requirement R1, Part 1.2

One commenter stated that the Draft 1: CIP-008-6 Requirement R4, Part 4.3 contained a parameter and not a requirement.
The SDT agrees and modified the wording in Part 4.3 (which is now Part 4.2)

One commenter stated that the term "compromise" and "disrupt" should be included in the entity definitions that same way "programmable" is.
The SDT asserts this is outside the scope of Project 2018-02.

Several commenters raised concerns about inconsistency with the use of Reportable Attempted Cyber Security Incident and the words determined within the Measures associated with Requirement R4.
The SDT removed the proposed Reportable Attempted Cyber Security Incident definition. Instead, the team leveraged the existing Cyber Security Incident definition, and modified the proposed CIP-008 R4, Part 4.2 language to qualify that attempts to compromise a system identified in the "Applicable Systems", including High Impact BES Cyber Systems and their associated EACMS and Medium Impact BES Cyber Systems and their associated EACMS, are reportable after the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2. As a result of these modifications, the M4 verbiage was modified to match.

Several commenters raised concerns that the proposed standard has the potential to create a significant auditing burden regarding "attempts to compromise," which have no impact on reliability.
The SDT asserts that the new requirement for reporting attempts to compromise (formerly defined as Reportable Attempted Cyber Security Incident in the first proposed draft) carries a similar evidence requirement for currently existing Reportable Cyber Security Incident.