NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-008-6

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

January 2019

RELIABILITY | ACCOUNTABILITY



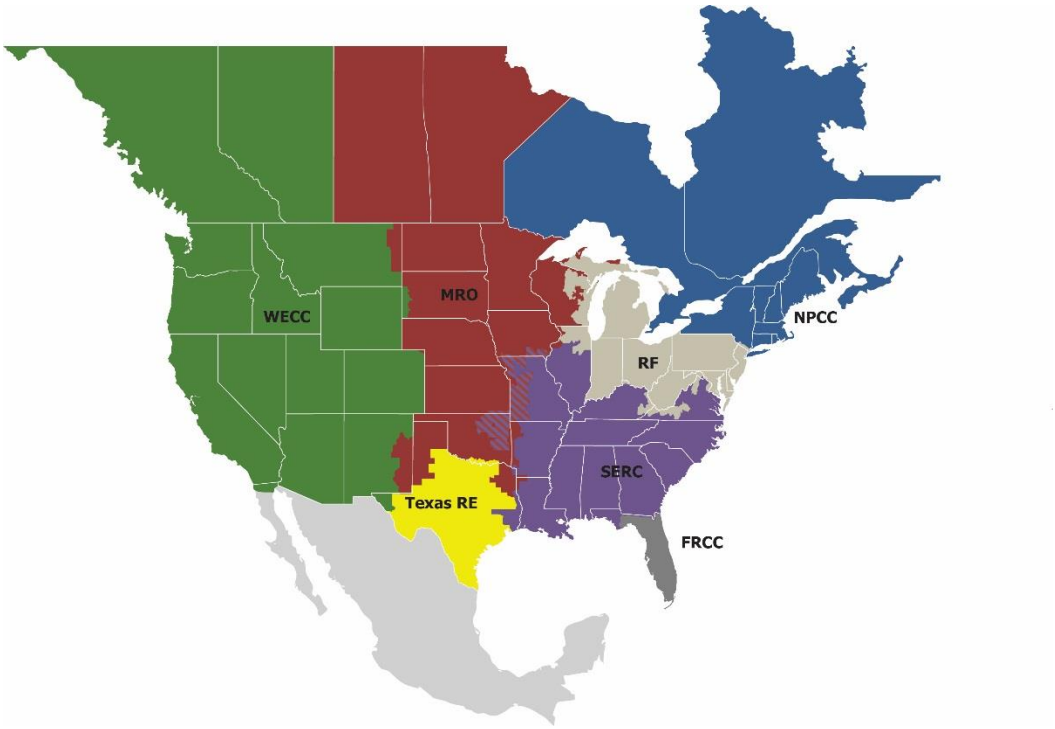

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

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 10-day public comment period, ending Thursday, November 29, 2018. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. 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.

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 requested the SDT modify the Cyber Security Incident definition to clarify it to include both disruption and compromise for all sub points the way the RCSI definition does.

The Cyber Security Incident definition includes: "compromises, or was an attempt to compromise" in its first bullet, and "disrupts, or was an attempt to disrupt," in its second bullet. The SDT asserts that both terms are addressed within the definition. The SDT was purposeful when associating compromise with the cyber systems and perimeters whereas disruptions are related to the function or reliability task. This distinction helps further clarify what is in scope for low impact BES Cyber Systems.

One commenter suggested adding PSP to RCSI 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. Cyber Security Incident that compromises or attempts to compromise a PSP would become reportable under the RCSI definition when it results in a compromise or disruption of one or more reliability tasks.

Commenters requested the SDT modify the Reportable Cyber Security Incident definition to delete "that performs one or more reliability tasks of a functional entity."

Thank you for your comment, the team asserts that the inclusion of the phrase "that performs one or more reliability tasks of a functional entity" in the Reportable Cyber Security Incident definition adds additional clarity and has elected to leave it in the proposed definition. In addition, it is consistent with previous versions of CIP-008.

Several commenters expressed concern that low impact could be interpreted as in scope as a function of the Cyber Security Incident definition.

The SDT addressed this concern by moving "high and medium impact" in front of BES Cyber Systems and ESP, PSP and EACMS in the first bullet of the Cyber Security Incident definition. The SDT asserts this single change also addresses the concern for the Reportable Cyber Security Incident definition.

Some commenters requested that the SDT modify the RCSI definition to include reportable attempts.

The SDT understands there could be some confusion, but the team strived to strike a balance between clear reporting definitions and timeframes commensurate with risk related to reporting attempts and RCSI. The SDT asserts that a change to the RCSI definition could affect more than CIP-008 and have consequences relative to CIP-003.

One commenter asserted that the definition of the revised terms was not provided.

The SDT thanks you for your comment. The revised terms were provided in the New or Modified Term(s) Used in NERC Reliability Standards section of the draft standard.

Reporting

While the majority of the commenters appreciated the extended notification timeframes provided in Requirement 4, Parts 4.2 and 4.3, several commenters again requested the inclusion of CIP Exceptional Circumstances (CEC).
The SDT foremost asserts that a general review of CEC is ongoing as part of the scope of Project 2016-02. The SDT further asserts that waiving the notification requirements when faced with a situation that involves or threatens to involve an imminent or existing hardware, software, or equipment failure, or a Cyber Security Incident requiring emergency assistance, is in direct contradiction to the intent of FERC Order No. 848. It is in exactly these types of situations where it is most important to share information amongst sector entities to stave off similar threats to protect the reliability of the BES.

Several commenters stated that the notification timeframes were confusing, inappropriate for updated information, or unduly burdensome. Also, a concern was raised that specifying a specific number of days for reporting actual and attempted Cyber Security Incidents to agencies will sometimes be a resource challenge. The recommendation is that the SDT consider a time frame that provides an update within 24 hours of actual determination of the criteria established in R4.1.
The SDT asserts that it is within each entity's purview to define its own criteria for and determination of reportability and knowledge of attributes. Throughout the requirement compliance timing begins with each determination as the entity executes its response process. It is upon the entity's determination that the notification timeframes are predicated — whether it is one hour from determination that an attempt to compromise is now a Reportable Cyber Security Incident, or whether it is within seven days after the determination of new attribute information. It is not the SDTs intent for an entity to rush their incident response process. Initial notifications can be preliminary and include only information that is known at the time of determination. Additional attribute information that is determined as the investigation continues should be reported per the update timeframes in the standard.

A commenter requested that the notification timeframes be consistent for Parts 4.2 and 4.3, specifically seven days after determination for an initial notification, as well as updates.
The SDT asserts that seven days after determination for an initial notification is not an appropriate reporting threshold. The reporting timeline for attempts to compromise is in alignment with FERC Order No. 848, p 89 and is in the spirit of timely reporting for information sharing. In addition, the one-hour initial notification timeframe for Reportable Cyber Security Incidents is not new and entities should already have processes in place to satisfy that requirement.

A commenter expressed concern about reporting to two different agencies and requested doubling the timeframe for initial notification to accommodate the additional agency reporting requirement.
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.

Several commenters requested coordination amongst the electric sector's event notification requirements, i.e., U.S. Department of Energy (OE-417), EOP-004, and CIP-008. Also, some commenters would like to leverage reporting to E-ISAC as an intermediary to NCCIC.
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.

The SDT asserts that the proposed reliability standard is responsive to FERC Order 848 and that E-ISAC acting as an intermediary is outside of the scope of the SAR.

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.

Many of the commenters, expressed the desire to have a Standardized Reporting form and to submit one report for automatic submission to the two entities.
While the initial form that was developed is not required, it is included as an example in Implementation Guidance and available for use. The SDT has preserved the entity's ability to choose to use that form or not.

One commenter expressed concern that auditor will use subjective judgement.
Thank you for your comment. The SDT wanted to give flexibility to entities in creating their process to accommodate differing size entities while meeting the requirements in the FERC order. The SDT has been working in close collaboration with the RSAW Task Force developing the CIP-008-6 RSAW.

One commenter stated that Part 4.2 stands on its own and 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.
This concern has been addressed by adding clarifying language to each of the applicable parts. It is not the intent of the SDT to infer that all Cyber Security Incidents are reportable. Rather, the SDT has developed standards requirement language that provides entities with the flexibility to create processes and criteria to ascertain what is reportable.

EACMS and Scoping

Two commenters asked that the SDT limit EACMS in the applicable systems column to exclude systems solely performing monitoring functions.
The SDT reevaluated FERC Order No. 848 and asserts that two of the five functions listed within the directive in Paragraph 54 (monitoring and logging, and alerting) are intentionally included.

One commenter stated that 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.
The SDT removed the mention of the five functions within the standard and the current definition of EACMS stands. 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.

One commenter disagrees with the inclusion of EACMS.
Thank you for your comment, the SDT asserts that EACMS is include per FERC order 848 Paragraph 54.

One commenter requested the SDT add ESPs to Applicable Systems in R1.2.2 and R4.2.
The SDT thanks you for your comment. The applicable systems in the proposed standard meet FERC Order 848 for the systems to be included.

Some commenters expressed concern that attempts to compromise potentially expand the scope to assets that are corporate systems or otherwise not associated with the CIP program.

The SDT added clarifying language to both the definitions and requirements in an effort to ensure that the scope was limited to the appropriate Applicable Systems.

Requested Modifications to Standard Language

Several commenters requested that the SDT define attempts to compromise, define criteria for attempts to compromise; or define a minimum set of criteria for attempts to compromise.

The SDT thanks commenters for their input. 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 to compromise", as well as defining criteria for "attempts to compromise;" or defining a minimum set of criteria for "attempts to compromise."

The SDT further asserts that no two Responsible Entities are alike and the determination of "attempts" and criteria for "attempts" is contextual and dependent on what is normal within each unique organization.

To define "attempt" or criteria for "attempts" 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.

In order to futureproof the standard the SDT determined that it was not to the benefit of Responsible Entities to define any fixed sets of criteria for "attempts to compromise" based on :

- The current state of cyber security threats will continue to evolve and that the associated security technologies will also evolve in response to these threats. The criteria for "attempts to compromise" will also evolve over time as a result

- Embedding criteria based on current technical requirements (such as those from CIP-007-6 R4.1) and/or direct references to other CIP standards such as CIP-007-6 R4.1 creates an administrative issue when changes to those technical requirements or the referenced standards are required.

The SDT has developed proposed Implementation Guidance inclusive of several examples in an effort to address this.

The team received comments stating that they appreciate the flexibility to establish our own criteria, they 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.

The SDT thanks you for your comment. The SDT strived to strike a balance between flexibility and consistency in the standard. The SDT believes this meets FERC order 848 and provides flexibility in implementation and future proofs the standard. This approach reflects the approach taken in other current enforceable standards, whereby the entity defines the criteria that best meets their unique operating environment.

Some commenters stated that "attempts" have been a part of the definition for a Cyber Security Incident for more than a decade and the entity does not support a process to define "attempts."

The SDT sought to create language that allows the entity flexibility to work the definition for attempts into their processes in a manner that supports the FERC order 848 reporting requirement directives and accommodates unique operating environments.

Many commenters recommend 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."

The SDT thanks you for your comments. The word "only" has been removed from the final version of the standard.

One commenter stated that referring to the "Applicable Systems" column within the "Requirements" column was redundant and confusing.

The SDT asserts that this reference provides additional clarity for the narrowed scope of reportable attempts to compromise.

Some comments were received regards to the structure of Requirements R1.1 and R1.2. It was suggested that R1.1 include having a process and using it.
The SDT thanks commenters for their input. The SDT structured R1.1 as the requirement to a have one or more processes and R1.2 as the required elements for the contents of these process or processes. Requirement R2.2 requires the use of the processes defined in R1.

Some comments received that suggested R1.2 language was not worded correctly.
The SDT thanks commenters for their input. The intent was R1.2 contains elements of what is required in R1.1. The SDT has made clarifying changes to the standard to address this concern.

One commenter suggested the use of "method" instead of "criteria" in R1.2.1.
The SDT considered whether wording using "method" was a less prescriptive than using "criteria". At this time, the SDT feels that these words are effectively equivalent. The SDT did make other changes to clarify the wording in R1.2.1.

Some comments were received that double jeopardy exists between Requirement R1.2.3 and R4.
The SDT structured R1.2.3 as a required element of the process(es) needed for Requirement R1.1.
R4 is the requirement that defines to whom reports are required, the attributes to be reported and the timelines required. R1.2.3 and R4 are cascaded requirements and do not create a double jeopardy.

One commenter would like to see the reporting of an "attempt" to also constitute a test of entity incident response plan in R2.
Thank you for your comment, the SDT intentionally excluded attempts to compromise from Requirement R2, Part 2.1. Please see Technical Rationale for justification.

PCAs

Some commenters indicated that PCAs should be included as part of the applicable systems.
The SDT thanks commenters for their input. The SDT has determined that the addition of PCAs to the applicable systems may create additional administrative burden given that:

- PCAs were not specifically discussed within FERC order 848, appearing only in P10 in reference to EACMS and ESP
- PCAs do not perform BES Reliability Operating Services that fall within the 15 minute criteria defined in CIP-002 and have a much lower risk profile
- While logging requirements are similar to BCS/BCA, PCA user authorization is currently not part of the CIP-004 program. While many entities already have existing user authorization programs for PCAs, adapting these existing programs into their CIP user authorization program may require extensive rework

The SDT asserts that entities retain the ability to voluntary report on PCA's as deemed appropriate and have added information to the Implementation Guidance to address this.

VRF/VSLs

Some commenters noted that some of the VSLs seem to be duplicative in the Severe and High columns for Requirement R4.
While the language is similar in both the High and Severe columns, the Severe uses "and" whereas the High uses "or." The intent was that if an entity failed to notify both E-ISAC and NCCIC, it violated the standard to a greater degree than only failing to notify one agency ("or") of a Reportable Cyber Security Incident.

Some commenters recommended the SDT consider how an auditor would interpret the standard to determine VSLs.
The SDT does not consider audit approach in determining VSLs. VSLs are one factor in assessing penalties after it has been determined the entity has violated the requirement. At that point, enforcement staff has reviewed the audit team's recommendations and determined that there has been a violation. When developing VSLs, the SDT considers whether an entity may still be in compliance with some parts of the requirement while violating others and assigns the VSLs accordingly.

Some commenters suggested moving the process to define attempts to compromise to a lower VSL than the process to identify Reportable Cyber Security Incidents and suggested putting other parts of Requirement R1 in the Lower and Moderate columns.
The SDT considered separating the tiers but ultimately determined not to change the severity level for attempts within Requirement R1. The SDT determined that the failure to include a process to define attempts or a process to identify Reportable Cyber Security Incidents in the Cyber Security Incident response plan are a similar degree of violation of Requirement R1. The SDT also determined that the other parts addressing the processes required to be included belonged in the Moderate column. Finally, the SDT determined not to lower the VSLs of some of the currently enforceable requirements from CIP-008-5.

Some commenters asserted that the VSLs do not appropriately reflect risk to BES reliability.
VSLs reflect degrees of compliance with the requirement, not risk to the BES. VRFs are indicators of impact to the BES if a requirement is violated. As the VRFs for R1 and R4 are Lower, the SDT asserts that they accurately reflect the risk of these administrative requirements.

One commenter noted that failure to notify the applicable agencies of an attempted Cyber Security Incident should not result in a severe penalty.
VSLs are just one factor in the determination of a penalty amount, so putting a requirement in the "Severe" VSL category does not necessarily mean that a Responsible Entity will receive a severe penalty. However, the particular violation the commenter describes would fall under the "Moderate" VSL category.

Some commenters noted that the 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" VRF to reflect the requirement's impact to reliability if violated. However, this consideration would not factor into how VSLs are determined.

Some commenters noted that they did not agree with the VSLs because of the requirement language or could not comment on the VSLs because of changes they recommended to the requirement language.
The SDT considered these comments when reviewing the requirement language.

One commenter noted that the shortened ballot period did not allow them to evaluate the VRFs or VSLs and another commenter noted disagreement with the VRFs and VSLs but did not think proposing alternatives would be considered.
The SDT understands this was a shortened comment period and ballot but appreciates industry's cooperation in meeting the 6-month deadline to file CIP-008-6 with FERC. Also, the SDT appreciates when commenters provide alternatives if in disagreement with the language.

Implementation Plan

A few comments were received that requested a 24 month implementation plan.

The SDT received comments regarding the timeframe for the Implementation Plan on the first ballot and the team adjusted from 12 to 18 months. The SDT assert that an 18-month implementation timeline is appropriate as it strikes a balance between the FERC directive for an expeditious implementation and capabilities of industry.

A few comments supported a 12 month implementation plan and one stated "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."

Based on the timing of Project 2016-02 and the current proposed changes, the SDT asserts that the net effect will not have significant impact on CIP-008-6.

One commenter asked what the SDT's intent for the initial performance of Part 2.1 and requested this be addressed in the Implementation Plan.

Thank you for your comment. The SDT chose not to include a section for the initial performance of certain period requirements in the interest of preventing confusion and in deference to the existing CAN-012 which clearly states, "[I]n the event that the standard or implementation plan is silent with regard to completing a periodic activity, CEAs are to verify that the registered entity has performed the periodic activity within the standard's timeframe after the enforceable date."

Cost Effectiveness

One commenter noted concern that the timelines for reporting may create additional administrative burden and cost.

The SDT understand there are cost considerations with every change to the standard. However, the SDT asserts, that the changes are not overly burdensome and balance added security, information sharing and the directives from the FERC order 848.

One commenter noted "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."

The SDT asserts that we made the fewest changes possible to meet FERC order 848. For example, the SDT removed the original proposed definition of Reportable Attempted Cyber Security Incident. The SDT also asserts that we carefully considered the impact to other standards to minimize the impact.

One commenter noted that the standard falls short in the area 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 scarce resources during an actual cyber security incident to focus attention on a duplicative task.

The SDT understands the concern about dual reporting but in order to meet the directives in FERC order 848, dual reporting is required. The SDT took efforts to ensure that entities could determine their methods of reporting in ways that minimize duplication of efforts such as co-copying on an email message**.** By giving the entity the ability to make their determination of when something is a Reportable Cyber Security Incident or an "attempt" the entity determines reporting clock start.

One commenter stated that the new standard ultimately requires Responsible Entities to become cyber security threat hunters rather than relying on the protections required within the CIP standards and requires investment in a 24x7x365 Security Operations Center (SOC). In addition, there is no reduction in risk to the BES in reporting attempts to compromise.

Thank you for your comment. The SDT asserts that the modifications do not require an entity to establish and implement a 24x7x365 Security Operations Center to achieve compliance, rather the entity may perform these activities on a schedule that is appropriate for their unique operating environment that is documented in their process. At a minimum, these modifications to this standard add formality around reporting for events that are detected and evaluated under existing enforceable standards with the intent to reduce risk to the BES through more timely information sharing and enhanced situational awareness that the expanded reporting will provide.

One commenter stated dependent upon what constitutes an "attempt", additional resources (personnel and/or tools) may be needed to investigate and report on attempted events.
The SDT asserts that the requirement has been written in a manner to provide the entity the flexibility to establish criteria and processes to determine what constitutes an attempt such that they may operate and achieve compliance in a cost effective way.

Some commenters noted that they could not comment on the cost effectiveness of the standard because of changes they recommended to the requirement language.
The SDT considered these comments when reviewing the requirement language.

One commenter expressed concerns with the scoping of the Standard Authorization Request process.
Thank you for your comment, the SDT asserts that the SAR, authorized by the Standards Committee was adequately scoped to meet the directives of FERC order 848. SAR development was prior to the establishment of the Standards Drafting Team (SDT).

Other

Some commenters expressed concern over the shortened timeframe of the project.
The SDT thanks you for your response. We understand that the accelerated timeline could have created a situation where comments were on a shorter timeframe. While there were some scheduling challenges the SDT did the best to balance the timeframe with industries availability. In addition, the standard drafting process requires NERC Board of Trustee approval before filing with FERC to meet order 848 deadline of April 1, 2019.

A comment was received that stated the comment form did not provide specific questions for every requirement and all supporting documentation.
Thank you for your comment. In an attempt to keep the comment form concise, the SDT offered questions on the comment form for the major changes from the previous draft of the standard. The SDT asserts that there is always an opportunity to respond to any area of the standard in the last "catch all" question.

On commenter stated that 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
The SDT thanks you for your comment. During this process the SDT worked closely with E-ISAC to discuss issues with them. While there are always issues with balancing information that is received, the E-ISAC provides opportunities to entities to adjust the way they are receiving information.

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.
The SDT thanks you for your comment, the Guidelines and Technical Basis will be included in its entirety within the TR and the IG for historical reference. It should also be noted that previous versions of the standards also contain this information and as standards are revised the GTB doesn't always match to the new updates.