Unofficial Comment Form

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Note that this comment period is 20 days, with the ballot pool forming the first 15 and the initial ballot conducted the final 5 days.

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to provide comments on CIP-008-6 — Cyber Security - Incident Reporting and Response Planning. Comments must be submitted by 8 p.m. Eastern, Tuesday, October 22, 2018.

Additional information is available on the project page. If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

Background Information
The purpose of this project is to address the directives issued by FERC in Order No. 848 in order to augment mandatory reporting of Cyber Security Incidents, including attempts that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would “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).” (Order No. 848 at P1)

Proposed Reliability Standard CIP-008-6 addresses the 4 elements outlined by FERC:

1. Responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity’s ESP or associated EACMS;

2. Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information;

3. Establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and

4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).
Questions

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

☐ Yes
☒ No

Comments:
Definitions do not limit what must be reported. Entity will need to devote significant resources to reporting – which takes away resources from addressing cyber attacks
Some concern with “Reportable Cyber Security Incident” for field locations (substations & generators) since these locations have fewer defense layers.
Concerns that the “Cyber Security Incident” puts the burden of determining intent – is the intent to “compromise” or “disrupt.” Expect this lack of clarity to result in in over-reporting which makes finding the real incident akin to a needle in the haystack.

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

☒ Yes
☐ No

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

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

☐ Yes
☒ No

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

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

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

☐ Yes
☒ No

Comments:

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

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

What about information protection when submitting?

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

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

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

☒ Yes
☐ No

Comments:

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

☐ Yes
☒ No

Comments:

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

We request clarification. ICS-CERT has its own process. Are Entities expected to add additional answers when submitting to ICS-CERT? If ICS-CERT changes its process, are Entities expected to follow that new CERT process when this Standard has not been updated?
7. Do you agree with the 12-month Implementation Plan? If you think an alternate, shorter, or longer implementation time period is needed, please propose an alternate implementation plan and time period, and provide a detailed explanation of actions planned to meet the implementation deadline.

☐ Yes
☐ No

Comments:

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

☐ Yes
☐ No

Comments:

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

Comments: