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

Please note that this comment period is 15 days, with the ballot conducted the final 10 days.

Do not use this form for submitting comments. Use the Standards Balloting and Commenting System (SBS) to submit comments on CIP-008-6 - Cyber Security — Incident Reporting and Response Planning by 8 p.m. Eastern, Thursday, November 29, 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) 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
☐ No

Comments:

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
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?

☑ Yes
☐ No

Comments:

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.
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.

☑ Yes
☐ No

Comments:
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 the Applicable Systems of tables R1 and R4.

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.

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.

☑ Yes
☐ No

Comments:
Agree
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
☐ No

Comments:
Agree

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:
Agree

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.

☐ Yes
☐ No

Comments:
Agree

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:
Abstain
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
☐ No

Comments:
Abstain

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

Comments:
No additional comment