Unofficial Comment Form

Project 2022-05 Modifications to CIP-008 Reporting Threshold

**Do not** use this form for submitting comments. Use the [Standards Balloting and Commenting System (SBS)](https://sbs.nerc.net/) to submit comments on **Project** **2022-05 Modifications to CIP-008 Reporting Threshold Standard Authorization Request (SAR).** Comments must be submitted by **8 p.m. Eastern, Monday, December 5, 2022.**

Additional information is available on the [project page](https://www.nerc.com/pa/Stand/Pages/Project2022-05ModificationstoCIP-008-aspx.aspx). If you have questions, contact Senior Standards Developer, [Alison Oswald](mailto:alison.oswald@nerc.net?subject=2022-05%20Modifications%20to%20CIP-008%20Reporting%20Threshold) via email), or at 404-446-9618.

## Background Information

Reliability Standard CIP-008-6 became effective on January 1, 2021, in response to FERC Order No. 848[[1]](#footnote-1) directing NERC to develop modifications to the Reliability Standards to require reporting of Cyber Security Incidents and attempt(s) to compromise a responsible entity’s Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS). In Q3 2021, the ERO Enterprise initiated a study to better understand how registered entities have implemented Reliability Standard CIP-008-6; specifically, how the registered entities have interpreted Reportable Cyber Security Incidents and defined attempt(s) to compromise. The study concluded that the current language of the Reliability Standard permits the use of subjective criteria to define attempt(s) to compromise, and most programs include a provision allowing a level of staff discretion. Reliability Standard CIP-008-6, or definitions, should be modified to provide a minimum expectation for thresholds defining attempt to compromise.

Since the effective date of CIP-008-6, there has not been a material change from CIP-008-5 in the number of Reportable Cyber Security Incidents or Cyber Security Incidents that were determined to be an attempt to compromise an applicable system. This project will address gaps in CIP-008-6 permitting a subjective determination of attempt(s) to compromise. The Standard Drafting Team (SDT) will modify the Reliability Standards and associated definitions as necessary to provide a minimum expectation for thresholds to support the definition of attempt to compromise.

## Questions

1. Do you agree with the proposed scope as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope, please provide your recommendation and explanation.

Yes

No

Comments:

1. Do you believe that other CIP standards will need to be modified for consistency to meet the goals laid out in the SAR? If so, please provide the standard recommendation and explanation.

Yes

No

Comments:

1. Provide any additional comments for the SAR drafting team to consider, if desired.

Comments:

1. <https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/E-1_Order%20No.%20848.pdf> [↑](#footnote-ref-1)