Unofficial Comment Form

Project 2023-04 Modifications to CIP-003

**Do not** use this form for submitting comments. Use the [Standards Balloting and Commenting System (SBS)](https://sbs.nerc.net/) to submit comments on draft four of Reliability Standard **CIP-003-11 –** **Cyber Security – Security Management Controls** by **8 p.m. Eastern, Thursday, October 10, 2024.
m. Eastern, Thursday, August 20, 2015**

Additional information is available on the [project page](https://www.nerc.com/pa/Stand/Pages/Project-2023-04-Modifications-to-CIP-003.aspx). If you have questions, contact Manager of Standards Development, Alison Oswald (via email), or at 404-275-9410.

## Background

## ​​​In light of cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact Bulk Electric System (BES) Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts who were representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The Standards Committee accepted the Standard Authorization Request (SAR) at its March 22, 2023 meeting.

The LICRT report recognized that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The LICRT recommended enhancing the existing low impact category to further mitigate the coordinated attack risk. The proposed project will revise CIP-003-9 to add electronic access controls to authenticate remote users, protect the authentication information in transit, and detect malicious communications for assets containing low impact BES Cyber Systems with external routable connectivity. ​

Please provide your responses to the questions listed below, along with any detailed comments.

Questions

1. Do you agree with the language proposed in CIP-003-11 Attachment 1? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. Do you agree with the language proposed in CIP-003-11 Attachment 2? If you do not agree, please explain why and provide recommended language you would support and, if appropriate, technical, or procedural justification.

[ ]  Yes

[ ]  No

Comments:

1. The Drafting Team (DT) proposes a three (3) year implementation plan for CIP-003-11. Do you agree with the proposed implementation plan? If you think an alternate timeframe is needed, please propose an alternate implementation plan with a detailed explanation.

[ ]  Yes

[ ]  No

Comments:

1. The DT believes the language of CIP-003-11 addresses the issues outlined in the SAR 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:

1. Do you have any concerns in the way Project 2023-04 made conforming changes to CIP-003-11 to align with virtualization changes in Project 2016-02?

[ ]  Yes

[ ]  No

Comments:

1. Provide any additional comments on the standard and technical rationale for the DT to consider, if desired.

Comments: