MAR 8, 2023

NERC CIP Standards Update

ieso
Connecting Today. Powering Tomorrow.

Contents

Summary of SDT Activities

Details of SDT Activities

Other Items

New CIP Standards Coming into Effect

ieso
Connecting Today. Powering Tomorrow.

Summary of Active NERC SDTs

Project 2016-02 CIP Mods SDT - Planning to issue Draft 5 at end of March of only CIP-005-8 and CIP-010-5. The other Draft 4 CIP standards passed Ballot 4

Project 2020-03 SDT Supply Chain Low Impact SDT – CIP-003-9 submitted to FERC on Dec 6, 2023

Project 2020-04 SDT CIP-012-2 – Cyber Security – Communications between Control Centers - Failed on drafted availability requirements. Call for new additional SDT members to replace existing members that have retired.

Summary of Active NERC SDTs

Project 2021-03 SDT TOCC CIP-002 / CIP-014 – changes to address TO Control Centers , IROL language changes and define classification of EACMS, PACS and PCAs – comments to 2 draft SARs submitted, New SAR submitted, TOCC Field Test completed

Project 2022-05 Modifications to CIP-008 Reporting Threshold – Changes to CIP-008-6 to a define a minimum criteria to evaluate and define "attempts to compromise" cyber security incidents. Comments to draft SAR submitted

Details - Project 2016-02 SDT CIP Modifications

- Addresses virtualization and V5TAG recommended changes
- Draft 5 proposed posting end of March 2023 , 45 day review
- Likely posting the 2 CIP standards that did not pass
- CIP-005-8 (Electronic Security Perimeters)
- CIP-010-5 (Change Control)

ieso
Connecting Today. Powering Tomorrow.

Project 2016-02 SDT CIP Modifications

- CIP-005-8 strategy: Clarify capability vs. intent for Interactive Remote Access, clarify serial port connectivity, clarify virtualization sharing rules for applicable systems outside the Electronic Security Perimeter (ESP)
- CIP-010-5 strategy: Retain objective language allowing flexibility for entities to develop their own change control methodology, avoid prescriptive baseline requirements.
- Next ballot likely late March 2023

Project 2020-04 CIP-012 Mods SDT

- This SDT address changes to CIP-012-1 Communications between Control Center to add availability requirements
- Draft 3 failed ballot at = 57.8%
- Call for additional new drafting team members as some existing drafting team have retired.
- Main contention is around what “availability” means.
- IRC suggested method to address “availability” issue appears to be viable

Project 2020-03 Supply Chain Low Impact SDT

- This SDT was for changes to address detection of malicious communications for vendor electronic remote access
- Final ballot passed on Nov 7 at 68.9% , adopted by NERC BOT on Nov 16, submitted to FERC on Dec 6, 2022 as CIP-003-9 (RD23-3-000)
- Note that there is an interaction between CIP-003-9 and changes to CIP-010-5 for handling of Transient Cyber Assets.

ieso
Connecting Today. Powering Tomorrow.

Project 2021-03 SDT TOCC CIP-002/CIP-014

- This project addresses SARs for Transmission Owner Control Centers; Interconnection Reliability Operating Limit (IROL) and Cyber Asset Classifications (EACMS, PACS, PCA)
- Comments submitted on 2 draft SARs, awaiting next draft. Existing SAR requires no comments
- A new SAR was posted requesting exemption changes for protocol converters . Comments yet to be submitted – likely to be changed to a RFI

ieso
Connecting Today. Powering Tomorrow.

Project 2021-03 SDT TOCC CIP-002/CIP-014

- TOCC Field Test Results – it may be appropriate to incorporate additional inclusion characteristics into the (CIP-002-5.1 Attachment 1) Criterion 2.12 and the previously proposed aggregate weighted value.
- Such inclusion characteristics include control of Transmission Facilities associated with a major interface or Blackstart Resources and initial Cranking Paths.
- Further, it may also be appropriate to incorporate exclusion criteria, recognizing that some Control Centers whose aggregate weighted value of lines exceeds 6000 may have a negligible impact on the reliability of the BES, if compromised.

Project 2022-05 SDT CIP-008 Reporting Threshold

- This SDT would add minimum criteria for the evaluation and definition of "attempts to compromise".
- Modify CIP-008-6 R1 Part 1.2.1 to read, "...That include criteria to evaluate and define attempts to compromise *which include, at a minimum, each of the following types of cyber security incidents:… "*
- Comments submitted, awaiting next SAR draft
- Note possible interaction with the US CISA RFI issued on Sept 9, 2022 – proposing mandated cyber incident reporting requirements.

Other Items

FERC Order RD23-2-000 issued Dec 15, 2022 directing NERC to conduct a study evaluating the effectiveness of Reliability Standard CIP-014-3 and submit the report within 120 days .

This is in response to the recent physical attacks on transformer stations and in particular, the attack in Moore County NC that resulted in a prolonged outage. CIP-014-3 covers physical protection of critical BES transmission system components . It is currently is not applicable to IESO, only Hydro One.

It is anticipated that FERC may order extending CIP-014 protections other critical BES assets such as control centers belonging to Reliability Operators, Balancing Authorities, etc.

Other Items

FERC Order RM22-3-000 issued on Jan 19, 2023 on Internal Network Security Monitoring requiring NERC to modify CIP Standards within the next 15 months for High and Medium impact BES Cyber Systems with External Routable Connectivity. NERC is also ordered to evaluate the same protection for Low impact and remaining Medium impact BES Cyber Systems within 12 months

Note that CIP-003-9 (submitted to FERC) already requires monitoring of remote vendor communications to Low impact BES Cyber Systems. This order may eventually extend monitoring to all network activity associated with Low impact BES Cyber Systems

Other Items

Proposed Changes to NERC Standards Process

- The goal is to produce faster turnaround times for changes to NERC Standards, in particular for CIP Standards
- Current standards process follows the ANSI standards process
- Combine the Standards Authorization Request (SAR) drafting team and Standards Drafting Team (SDT) together
- Shorter ballot periods
- More use of informal industry feedback
- Eliminate Final Ballot

Other Items

US Federal Government National Cybersecurity Strategy (NCS) - Biden Administration announced a National Cybersecurity Strategy on March 22, 2023

It appears that EPA (water sector) and DOE (electricity sector) will be the lead agencies in developing the National Cybersecurity Strategy with respect to cyber protections for critical infrastructure

It remains to be seen how the creation of this NCS will impact the NERC CIP Standards

New CIP Requirements

CIP-013-2, CIP-005-7 and CIP-010-4 standards to address supply chain requirements for PACS, EACMS came into effect on Oct 1, 2022

CIP-004-7 and CIP-011-3 BCSI in the Cloud changes comes into effect on Jan 1, 2024 (Note – early adoption is allowed to take advantage of these changes)

CIP-003-9 Vendor Electronic Remote Access Controls for Low Impact BCS (TBD - filed with FERC Dec 6, 2022 , 3 year implementation plan)

ieso
Connecting Today. Powering Tomorrow.

Thank You

ieso.ca

1.888.448.7777

customer.relations@ieso.ca

engagement@ieso.ca

@IESO_Tweets

facebook.com/OntarioIESO

linkedin.com/company/IESO

ieso
Connecting Today. Powering Tomorrow.