DEC 2022

# NERC CIP Standards Update

ieso
Connecting Today. Powering Tomorrow.

# Active NERC SDTs

Project 2016-02 CIP Mods SDT failed Ballot 4 of the V5TAG issues (Virtualization and External Routable Connectivity / Interactive Remote Access) changes to CIP-002 to CIP-013.

Project 2020-03 SDT Supply Chain Low Impact SDT – Passed final ballot of as CIP-003-9 and adopted by NEC BOT

Project 2020-04 SDT CIP-012-2 – Cyber Security – Communications between Control Centers - Failed Ballot 3 on availability requirements for communications links between Control Centers

# Active NERC SDTs

Project 2021-03 SDT TOCC CIP-002 / CIP-014 – changes to address :

- Transmission Owner Control Centers that perform functions of a Transmission Operator (CIP-002)
- (new) Define classification process of Electronic Access Control and Monitoring Systems (EACMS), Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA) (CIP-002)
- (new) Change wording related to Interconnection Reliability Operating Limit (IROL) as part of changes started by NERC Project 2015-09 – System Operating Limits (CIP-002 / CIP-014)

# Project 2016-02 SDT CIP Modifications

- Addresses virtualization and V5TAG recommended changes
- Draft 4 was posted on Aug 17, 2022. Ballot closed Nov 7, 2022
- CIP-005-8 (Electronic Security Perimeters) just barely failed 65.26%
- CIP-007-7 (System Hardening) just passed 67.38%
- CIP-010-5 (Change Control) failed 46.35%
- CIP-002, CIP-003, CIP-004, CIP-006, CIP-008, CIP-009, CIP-011, CIP-013 passed



ieso
Connecting Today. Powering Tomorrow.

# Project 2016-02 SDT CIP Modifications

| Standard | Quorum / Approval | Quorum / Supportive Opinions |
|---|---|---|
| CIP-002-7 | 77.12% / 94.63% | 80.00% / 97.25% |
| CIP-003-Y | 77.12% / 84.90% | 75.00% / 87.36% |
| CIP-004-8 | 77.30% / 84.60% | 80.00% / 88.46% |
| CIP-005-8 | 77.63% / 65.26% | 80.36% / 69.95% |
| CIP-006-7 | 77.30% / 92.60% | 79.72% / 93.44% |
| CIP-007-7 | 76.97% / 67.38% | 79.72% / 73.08% |
| CIP-008-7 | 76.97% / 95.67% | 79.72% / 96.70% |
| CIP-009-7 | 76.97% / 95.38% | 79.72% / 96.15% |
| CIP-010-5 | 77.30% / 46.35% | 79.72% / 57.46% |
| CIP-011-4 | 76.97% / 82.59% | 80.07% / 87.50% |
| CIP-013-3 | 76.97% / 82.88% | 79.72% / 87.98% |

# Project 2016-02 SDT CIP Modifications

- CIP-005-8 themes: Interactive Remote Access – Capability vs. Intent; IP network connectivity conversion to serial connectivity; Virtualization sharing rules for applicable systems outside the Electronic Security Perimeter (ESP)
- CIP-010-5 themes: Missing requirement for documentation on the entity determination of how it meets change control objectives; Automatic remediation interaction with Protected Cyber Asset (PCA) / Transient Cyber Asset (TCA) definitions
- Next ballot likely mid-late Jan 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%
- Main theme around what "availability" means. "Availability" should address the ability of the entity to perform it's reliability functions vs. the pure availability of data from other control centers
- This would allow entities to use other methods besides redundancy such as manual values, computed values, etc.



ieso
Connecting Today. Powering Tomorrow.

# Project 2020-03 Supply Chain Low Impact SDT

- This SDT was for changes to address detection of malicious communications for vendor electronic remote access
- Ballot for Draft 3 as CIP-003-X passed ballot in August 19, 2022 at 66.81%
- As 2016-02 SDT CIP-002-Y did not pass ballot, CIP-003-X went to final ballot as CIP-003-9.
- Final ballot passed on Nov 7 at 68.9% and adopted by NERC BOT on Nov 16



ieso
Connecting Today. Powering Tomorrow.

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

- This project addresses 3 SARs for Transmission Owner Control Centers; Interconnection Reliability Operating Limit (IROL) and Cyber Asset Classifications (EACMS, PACS, PCA)
- (existing SAR) TOCC – BES studies completed to determine if reclassifying some Medium Impact Control Centers to Low Impact is appropriate (CIP-002-6 was withdrawn for this topic)
- (new SAR) IROL language changes started by the 2015-09 System Operating Limits SDT need to be incorporated in CIP-002 and CIP-014
- (new SAR) There are no current requirements to classify EACMS, PACS and PCAs. As a result, any misclassification causes all non-compliance in all requirements



ieso
Connecting Today. Powering Tomorrow.

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

- TOCC and IROL language changes effect the dividing line between Low and Medium Impact BES Cyber Systems (Table in CIP-002 Attachment 1 Section 2)
- New requirements to classify EACMS, PACS and PCAs. This is to favorable to all entities. Failure to perform a single classification would only be a single requirement non-compliance in CIP-002. Currently, it is multiple non-compliances of all applicable requirements in all CIP Standards



ieso
Connecting Today. Powering Tomorrow.

# New SAR 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:… "*

# Other Items

FERC NOPR Incentives for Advanced Cybersecurity Investment; Cybersecurity Incentives issued Oct 16 – funding methods for new cyber security investments - does not effect IESO

US Cybersecurity and Infrastructure Security Agency (CISA) Request for Information (RFI) Sept 9, 2022 - Cyber incident reporting requirements, pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 - does not directly effect IESO, however may be reflected in future changes to CIP-008

# New CIP Requirements

CIP-013-2, CIP-005-7 and CIP-010-4 standards to address supply chain requirements for PACS, EACMS comes into effect 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 - yet to be filed with FERC, 3 year implementation plan)

# 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.