**2025 Annual Plan Items 3.a and 3.b Work Paper**

2025 WEQ Annual Plan Item 3.a – Review annually, at a minimum, WEQ-012 and the accreditation requirements for Authorized Certification Authorities to determine if any changes are needed to meet market conditions

2025 WEQ Annual Plan Item 3.b – Evaluate and modify standards as needed to support and/or complement the current version of the NERC Critical Infrastructure Protection Standards and any other activities of NERC and the FERC related to cybersecurity

NERC Activities

*Current Efforts Underway*

* [NERC Project 2023-06 CIP-014 Risk Assessment Refinement](https://www.nerc.com/pa/Stand/Pages/Project_2023-06_CIP-014_Risk_Assessment_Refinement.aspx)
  + Standard(s) Impacted: CIP-014 Physical Security
  + Purpose/Industry Need: As the intent of CIP-014-3 is to identify and physically protect those Transmission stations, Transmission substations, and their associated primary control centers that are critical to the reliable and secure operation of the BPS, registered entity approaches for the risk assessment must be reasonably consistent and substantiated with sufficient technically based rationale. There continues to be confusion within the industry as to how to adequately evaluate instability. Therefore, this project includes refinement of CIP-014 risk assessments to assure critical sites are identified and physically protected.
  + Status: [Draft 2](https://www.nerc.com/pa/Stand/202306_CIP014_Risk_Assessment_Refinement_DL/2023-06%20CIP-014-4_Redline%20to%20last%20posted_09232024.pdf) of CIP-014-4 posted for comment period ending November 6, 2024
* [Project 2021-03 CIP-002 Transmission Owner Control Centers](https://www.nerc.com/pa/Stand/Pages/Project%202021-03%20CIP-002%20Transmission%20Owner%20Control%20Centers.aspx)
  + Standard(s) Impacted: CIP-002 BES Cyber System Categorization and CIP-014 Physical Security
  + Purpose/Industry Need:
    - Phase 1 – Review CIP-002 and evaluate the categorization of Transmission Owner Control Centers (TOCCs) performing the functional obligations of a Transmission Operator
    - Phase 2 – Revise CIP-002 and CIP-014 to clarify the responsibility of Reliability Coordinators, Planning Coordinators, and Transmission Planners in identifying Facilities that warrant consideration under these Reliability Standards
  + Status:
    - Phase 1 – [CIP-002-8](https://www.nerc.com/pa/Stand/Project202103_CIP002_Transmission_Owner_Control_Ce/2021-03%20CIP-002-8_Redline_To_Last_Approved_FB_111324.pdf) approved by NERC BoT and filed with FERC in December 2024
    - Phase 2 – Anticipated start date Q1, 2025
* [Project 2023-09 Risk Management for Third-Party Cloud Services](https://www.nerc.com/pa/Stand/Pages/Project-2023-09-Risk-Management-for-Third-Party-Cloud-Services.aspx)
  + Standard(s) Impacted: CIP-002 through CIP-014
  + Purpose/Industry Need: The project purpose is to establish risk-based, outcome-driven requirements that place cloud services on par with other third-party resources already used for CIP-regulated systems including for BES operations and supporting cyber assets. This project will allow, but not require, use of cloud services for CIP-regulated systems including BES operations and supporting cyber assets. The goals are to develop specific modifications to the CIP Standards, or create a new standard(s), to add clarity in allowing for the adoption and auditability of cloud services used for the BES. These revisions will increase reliability and security to the Bulk Electric System (BES) by allowing the use of advanced technologies that support Entities in managing grid modernization and the changing grid landscape as well as making available to security teams all resources that can reduce potential impact and speed recovery from security events.
  + Status: [Standards Authorization Request](https://www.nerc.com/pa/Stand/202309RiskMgmtforThirdPartYCloudServices_DL/2023-09_Cloud%20Services%20SAR%20revised%20clean%20final_121024.pdf) accepted December 2024
* [Project 2022-05 Modifications to CIP-008 Reporting Threshold](https://www.nerc.com/pa/Stand/Pages/Project2022-05ModificationstoCIP-008-aspx.aspx)
  + Standard(s) Impacted: CIP-008
  + Purpose/Intent: In Q3 2021, NERC 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 resulting white paper concluded that​ Reliability Standard CIP-008-6, or definitions, will be modified to provide a minimum expectation for thresholds defining attempt to compromise.
  + Status: [Standards Authorization Request](https://www.nerc.com/pa/Stand/Project202205ModificationstoCIP008DL/2022-05%20CIP-008%20SAR%20-%20CLEAN_SC%20approved_071923.pdf) accepted July 2023

*Filed with FERC*

* [CIP-002-8 – Cyber Security – BES Cyber System Categorization](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-8.pdf)
  + December 20, 2024 in Docket No. RM25-7-000
  + Purpose: Would advance reliability by revising the “bright-line” criteria for applicable Transmission Owners and Transmission Operators to categorize their BES Cyber Systems based on the impact to their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System
  + Participants agreed likely no impact; no standard revisions needed at this time
* [CIP-003-11 Cyber Security – Security Management Controls](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-11.pdf)
  + December 20, 2024 in Docket No. RM25-8-000
  + Purpose: mitigate the risks posed by a coordinated attack utilizing distributed low impact BES Cyber Systems by adding controls to authenticate remote users; protecting the authentication information in transit; and detecting malicious communications to or between assets containing low impact BES Cyber Systems with external routable connectivity
  + Participants agreed likely no impact; no standard revisions needed at this time

**FERC Action**

* [FERC NOPR](https://elibrary.ferc.gov/eLibrary/) re: [NERC CIP-015-1](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-015-1.pdf) – Cyber Security – Internal Network Security Monitoring
  + FERC proposes to approve CIP-015-1 and proposes to direct NERC to develop certain modifications to extend internal network security monitoring to include electronic access control or monitoring systems and physical access control systems outside of the electronic security perimeter
  + September 19, 2024 in Docket No. RM24-7-000
  + Participants agreed likely no impact; no standard revisions needed at this time
* [FERC NOPR](https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20240919-3019) re: Supply Chain Risk Management Reliability Standards Revisions
  + FERC proposes to direct NERC to develop and submit for approval new or modified Reliability Standards addressing supply chain risk management, specifically supply chain risk management plan requirements regarding the identification, assessment, and response to supply chain risks
  + September 19, 2024 in Docket No. RM24-4-000
  + March 20, 2025 FERC-NERC Supply Chain Risk Management Reliability Standards Revisions [Workshop](https://ferc.gov/news-events/events/workshop-supply-chain-risk-management-reliability-standards-02242025)
  + Tie-in to 2025 WEQ Annual Plan Item 3.d
  + Participants agreed no standard revisions needed at this time but could be area of coordination

**Other Cybersecurity Activities**

* CA/B Forum activities
* Changes to the acceptance of code-signing certificates
* NIST Post-Quantum Encryption Algorithms; need to evaluate potential changes related to 2030 deprecation of RSA as part of 2026 review
  + [FIPS 203](https://doi.org/10.6028/NIST.FIPS.203) Module-Lattice-Based-Key Encapsulation Mechanism
  + [FIPS 204](https://doi.org/10.6028/NIST.FIPS.204) Module-Lattice-Based Digital Signature
  + [FIPS 205](https://doi.org/10.6028/NIST.FIPS.205) Stateless Hash-Based Digital Signature

NERC CIP Reliability Standards

Reliability Standards Subject to Enforcement

* [CIP-002-5.1a](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf) Cyber Security – BES Cyber System Categorization
* [CIP-003-8](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-8.pdf) Cyber Security – Security Management Controls
  + [CIP-003-9](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-9.pdf) Effective April 1, 2026
* [CIP-004-7](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-004-7.pdf) Cyber Security – Personnel & Training
* [CIP-005-7](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-7.pdf) Cyber Security – Electronic Security Perimeter(s)
* [CIP-006-6](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-006-6.pdf) Cyber Security – Physical Security of BES Cyber Systems
* [CIP-007-6](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-6.pdf) Cyber Security – System Security Management
* [CIP-008-6](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf) Cyber Security – Incident Reporting and Response Planning
* [CIP-009-6](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-009-6.pdf) Cyber Security – Recovery Plans for BES Cyber Systems
* [CIP-010-4](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-4.pdf) Cyber Security – Configuration Change Management and Vulnerability Assessments
* [CIP-011-3](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-011-3.pdf) Cyber Security – Information Protection
* [CIP-012-1](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-012-1.pdf) Cyber Security – Communications between Control Centers
  + [CIP-012-2](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-012-2.pdf) Effective July 1, 2026
* [CIP-013-2](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-2.pdf) Cyber Security – Supply Chain Risk Management
* [CIP-014-3](https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-3.pdf) Cyber Security – Physical Security