2023 WEQ Annual Plan Items 3.a and 3.b Work Paper

**NERC Activities**

*Current Efforts Underway*

* [NERC Project 2016-02 – Modifications to CIP Standards](https://www.nerc.com/pa/Stand/Pages/Project%202016-02%20Modifications%20to%20CIP%20Standards.aspx)
  + Issues that will be addressed are:
    - Cyber Asset and BES Cyber Asset Definition
    - Network and Externally Accessible Devices
    - Transmission Owner Control Centers Performing Transmission Operator Obligations
    - Virtualization
  + Standards impacted: CIP-002-7, CIP-003-9, CIP-004-7, CIP-005-8, CIP-006-7, CIP-007-7, CIP008-7, CIP-009-7, CIP-010-5, CIP-011-3, CIP-013-3
    - NERC formal comment period for the CIP Virtualization suite of standards closed October 10, 2022
* [Project 2020-03 Supply Chain Low Impact Revisions](https://www.nerc.com/pa/Stand/Pages/Project_2020-03_Supply_Chain_Low_Impact_Revisions.aspx)
  + Intent to modify CIP-003 to include policies for low impact BES Cyber Systems to:
    - Detect known or suspected malicious communications for both inbound and outbound communications
    - Determine when active vendor remote access sessions are initiated
    - Disable active vendor remote access when necessary
  + Standards impacted: CIP-003-8
    - NERC 45 day formal comment period on the standard open through April 15, 2022
* [Project 2020-04 Modifications to CIP-012](https://www.nerc.com/pa/Stand/Pages/Project202004ModificationstoCIP-012.aspx)
  + Addresses FERC directive in Order No. 866 to develop modifications to the reliability standards to require protections regarding the availability of communication links and data communicated between the bulk electric system Control Centers
  + Standards impacted: CIP-012
    - Supplemental drafting team nominations end February 2, 2023
* [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)
  + Addresses additional modifications that may be needed regarding the applicability of requirements to control centers.
  + Standards impacted: CIP-002
    - NERC 30 day formal comment period ended December 21, 2022
* [Project 2022-05 Modifications to CIP-008 Reporting Threshold](https://www.nerc.com/pa/Stand/Pages/Project2022-05ModificationstoCIP-008-aspx.aspx)
  + Addresses standard modifications and associated definition changes as necessary to provide a minimum expectation for thresholds to support the definition of attempt to compromise. Reliability Standard CIP-008-6, or definitions, will be modified to provide a minimum expectation for thresholds defining attempt to compromise.
  + Standards impacted: CIP-008

*NERC Guidelines*

* [Cyber Security Risk Management Lifecycle](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cyber_Security_Risk_Management_Lifecycle.pdf)
* [Open Source Software](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Risk_Considerations_Open_Source_Software.pdf)
* [Supply Chain Procurement](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Supply_Chain_Secure_Equipment_Delivery.pdf)
* [Vendor Incident Response](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Vendor_Incident_Response.pdf)
* [Cloud Computing](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cloud_Computing.pdf)
* [Vendor Risk Management Lifecycle](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Vendor_Risk_Management_Lifecycle.pdf)
* [Provenance](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Provenance.pdf)
* [Primer for Cloud Solutions and Encrypting BCSI](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline_BCSI_Cloud_Encryption.pdf)

*NERC Finalized Standards*

* CIP-003-9
  + Modifications from the past version include requirements applicable to low impact BES Cyber Systems and require a responsible entity to implement cyber security plans for low impact BES Cyber Systems that address the following areas:
    - Cyber security awareness
    - Physical security
    - Electronic security
    - Cyber Security Incident response
    - Transient Cyber Asset and Removable Media malicious code risk management
    - Vendor electronic remote access security controls
  + [Filed](https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition_for_Approval_CIP-003-9_filing.pdf) with the FERC on December 6, 2022 in Docket No. RD23-3-000

**FERC Action**

* FERC Order Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems
  + Issued January 19, 2022 in Docket No. RM22-3-000; NOPR issued January 20, 2022
* FERC NOPR [Incentives for Advanced Cybersecurity Investment](https://www.ferc.gov/media/e-1-rm22-19-000)
  + Issued September 22, 2022 in Docket Nos. RM22-19-000 and RM21-3-000 – comments closed November 7, 2022
  + As part of NOPR, FERC “proposes to revise its regulations to provide incentive-based rate treatments for the transmission of electric energy interstate commerce and the sale of electricity energy at wholesale in interstate commerce by utilities for the purpose of benefitting consumers by encouraging investments by utilities in advanced cybersecurity technology and participation by utilities in cybersecurity threat information sharing programs, as directed by the Infrastructure Investment and Jobs Act of 2021”
  + Per the NOPR, cybersecurity products “can include but are not limited to, security information and event management systems, intrusion detection systems, anomaly detection systems, encryption tools, data loss prevention systems, forensic toolkits, incident response tools, imaging tools, network behavior analysis tools, access management systems, configuration management systems, anti-malware tools, user behavior analytic software, event logging systems, and any system for access, control, identification, authentication, and/or authorization control.
  + Per the NOPR, cybersecurity systems “may be either automated or manual and can include, but are not limited to, system installation and maintenance, network administration, asset management, threat and vulnerability management training, incident response, forensic investigation, network monitoring, data sharing, data recovery, disaster recovery, network restoration, log analytics cloud network storage, and any general cybersecurity consulting service”

**Other Cybersecurity Activities**

* [Executive Order on Improving the Nation’s Cybersecurity](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/) (May 12, 2021)
* [Cyber Incident Reporting for Critical Infrastructure Act of 2022](https://www.congress.gov/bill/117th-congress/house-bill/2471/text)