2022 WEQ Annual Plan Items 4.a and 4.b Work Paper

**NERC Activities**

* [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 45 day formal comment period for the CIP Virtualization suite of standards open through April 11, 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-003-8 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
		- NERC holding 45 day comment period ended on January 24, 2022
* [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.
	+ CIP-002
* NERC Guidelines
	+ [Cyber Intrusion Guide for System Operators](https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Cyber_Intrusion_Guide_for_System_Operators_approved.pdf)
	+ [Cloud Computing](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline-Cloud_Computing.pdf)
	+ [Primer for Cloud Solutions](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Security_Guideline_BCSI_Cloud_Encryption.pdf)

**FERC Final Orders**

* FERC [Letter Order](https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20211207-3062) Approving Reliability Standards CIP-004-7 and CIP-011-3
	+ Standards clarify “the protections required surrounding the use of Bulk Electric System Cyber System Information (BCSI)…[by requiring] an access management program to authorize, verify, and revoke provisioned access to BCSI as well as a documented process regarding BES Cyber Asset reuse and disposal.”
		- “NERC explains that registered entities currently control BCSI by managing access to the “designated storage location” of BCSI, such as an electronic document or physical file room, without addressing third-party cloud computing services, which have become an option for storing BCSI.”

**FERC NOPRs**

* [FERC NOPR](https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20220120-3046) Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems
	+ Docket No. RM22-3-000, issued January 20, 2022 – comments closed March 28, 2022
	+ FERC proposes to direct NERC to develop and submit new or modified reliability standards that require internal network security monitoring within a trusted Critical Infrastructure Protection networked environment for high and medium impact Bulk Electric System Cyber Systems

**FERC NOIs**

* [FERC Notice of Inquiry Re: CIP Reliability Standards Enhancements](https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/NOI%20Potential%20Enhancements%20to%20CIP.pdf)
	+ FERC seeks comment on whether the CIP Reliability Standards adequately address the following topics:
		- Cybersecurity risks pertaining to data security
		- Detection of anomalies and events
		- Mitigation of cybersecurity events
	+ FERC also seeks comment on the potential risk of a coordinated cyberattack on geographically distributed targets and whether Commission action including potential modifications to the CIP Reliability Standards would be appropriate to address such risk
	+ NOI based on FERC staff review of the NIST Cyber Security Framework and identification of certain topics addressed by the framework that may not be adequately addressed in the CIP Reliability Standards
	+ Initial comments were due August 24, 2020
	+ Reply comments were due September 22, 2020
* [FERC Notice of Inquiry Re: Supply Chain](https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Supply%20Chain%20Notice%20of%20Inquiry.pdf)
	+ FERC seeks comments on the potential risks to the Bulk Electric System posed by the use of equipment and services produced or provided by certain entities identified as risks to national security. In addition, the Commission seeks comments on strategies to mitigate any potential risks posed by such telecommunications equipment and services
	+ Initial comments were due November 23, 2020
	+ Reply comments were due December 22, 2020

**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/) – Issued May 12, 2021
* [Cyber Incident Reporting for Critical Infrastructure Act of 2022](https://www.congress.gov/bill/117th-congress/house-bill/2471/text)