**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-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, CIP-011-2, and CIP-012-1
  + CIP-002-6 – Cyber Security – BES Cyber System Categorization was approved by the NERC Board of Trustees and submitted to FERC for approval on June 12, 2020
* [NERC Project 2019-02 BES Cyber System Information Access Management](https://www.nerc.com/pa/Stand/Pages/Project2019-02BCSIAccessManagement.aspx)
  + Project intended to enhance BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information by providing a secure path towards utilization of modern third-party data storage and analysis systems
  + The project would also clarify the protections expected when utilizing third-party solutions (aka cloud)
  + Standards impacted: CIP-004-6 Cyber Security Personnel & Training, CIP-011-2 Cyber Security Information Protection
  + Proposed drafts of CIP-004-7 and CIP-011-2 circulated for initial comment/balloting with industry in January 2020
* [NERC Project 2019-03 Cyber Security Supply Chain Risks](https://www.nerc.com/pa/Stand/Pages/Project2019-03CyberSecuritySupplyChain-Risks.aspx)
  + Addresses FERC directives in Order No. 850 to modify standards to address Electronic Access Control or Monitoring Systems (EACMSs), specifically those systems that provide electronic access control to high and medium impact BES Cyber Systems
  + NERC is also considering revising the standards to address Physical Access Control Systems (PACSs) that provide physical access control (excluding alarming and logging) to high and medium impact BES Cyber Systems.
  + Standards impacted: CIP-005-6 Cyber Security Electronic Security Perimeters, CIP-010-3 Cyber Security Configuration Change Management and Vulnerability Assessments, and CIP-013-1 Cyber Security Supply Chain Risk Management
  + Proposed drafts of CIP-005-7, CIP-010-4, and CIP-013-2 circulated for initial balloting/comment with industry in January 2020
* [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
  + [SAR](https://www.nerc.com/pa/Stand/202003_Supply_Chain_Low_Impact_Revisions_DL/2020-03_Supply_Chain_LIR_SAR_04032020.pdf) comment period ended on June 3, 2020
* [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
  + [SAR](https://www.nerc.com/pa/Stand/Project202004Modifications%20to%20CIP012DL/2020-04_CIP-12%20Directive%20SAR_042020.pdf) comment period ended on June 11, 2020
* 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)

**FERC Final Orders**

* [FERC Order No. 866 Critical Infrastructure Protection Reliability Standard CIP-012-1 Cyber Security – Communications between Control Centers](https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Approving%20Reliability%20Standard%20CIP-012-1%20(Cyber%20Security%20%E2%80%93%20Communications%20between%20Control%20Centers).pdf)
  + As part of order, FERC approved [CIP-012-1](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-012-1&title=Cyber%20Security%20%E2%80%93%20Communications%20between%20Control%20Centers)
  + These standards “support situational awareness and reliable bulk electric system operations by requiring responsible entities to protect the confidentiality and integrity of real-time assessment and real-time monitoring data transmitted between bulk electric system control centers.”
  + Also directed NERC to develop additional standards (see NERC Project 2020-04)

**FERC NOPRs**

* None to date

**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 due August 24, 2020
  + Reply comments due September 22, 2020