NERC Reliability Standards Under Development

* [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
* [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
* [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

FERC Final Orders

* [FERC Order No. 850 Supply Chain Risk Management Reliability Standards](https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20No.%20850%20Supply%20Chain%20Risk%20Management%20Reliability%20Standards.pdf)
  + As part of the order, the FERC approved:
    - [CIP-005-6 Cyber Security Electronic Security Perimeters](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-005-6&title=Cyber%20Security%20%E2%80%94%20Electronic%20Security%20Perimeter(s))
    - [CIP-010-3 Cyber Security Configuration Change Management and Vulnerability Assessments](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-010-3&title=Cyber%20Security%20%E2%80%94%20Configuration%20Change%20Management%20and%20Vulnerability%20Assessments)
    - [CIP-013-1 Cyber Security Supply Chain Risk Management](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-013-1&title=Cyber%20Security%20-%20Supply%20Chain%20Risk%20Management)
  + These standards “are forward-looking and objective-based and require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations, and consistent with FERC Order No. 829, the standards “focus on the following four security objectives: (1) software integrity and authenticity; (2) vendor remote access protections; (3) information system planning; and (4) vendor risk management and procurement controls
  + FERC also included directives for additional NERC action being addressed under NERC Project 2019-03
* [Letter Order Approving CIP-008-6](https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/Order%20Docket%20No.%20RD19-3-000.pdf)
  + FERC approved [CIP-008-6 Cyber Security Incident Reporting and Response Planning](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-008-6&title=Cyber%20Security%20%E2%80%94%20Incident%20Reporting%20and%20Response%20Planning)
  + These standards “require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity’s Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).”
* [Letter Order Approving CIP-003-8](https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/RD19-5-000%20Letter%20Order%20CIP-003-8.pdf)
  + FERC approved [CIP-003-8 Cyber Security Security Management Controls](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-003-7&title=Cyber%20Security%20%E2%80%94%20Security%20Management%20Controls)
  + These standards “specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to mis-operation or instability in the bulk electric system.”
  + NERC filed the petition in response to FERC Order No. 843 to develop modifications to the standards to mitigate the risk of malicious code that could result from third-party transient electronic devices for low impact BES Cyber Systems

FERC NOPRs

* [NOPR to Approve Reliability Standard CIP-012-1](https://www.nerc.com/FilingsOrders/us/FERCOrdersRules/NOPR%20CIP-012-1.pdf)
  + In FERC Order No. 822, the FERC directed NERC “develop modifications to require responsible entities to implement controls to protect, at a minimum, communication links and sensitive bulk electric system data communicated between bulk electric system Control Centers in a manner that is appropriately tailored to address the risks posted to the bulk electric system by the assets being protected.”
  + [CIP-012-1](https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-012-1&title=%20Cyber%20Security%20%E2%80%93%20Communications%20between%20Control%20Centers) “supports 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.”