What are the NERC CIP Reliability Standards?

The main goal of the NERC Critical Infrastructure Protection (CIP) Reliability Standards is to safeguard the integrity of the utility infrastructure in North America, especially for assets connected to IT systems.

Should the North American utility infrastructure become compromised by a cyberattack, millions of people would be affected by the limited availability of utilities such as:

- Transportation (e.g., local and interstate trains)
- Telecommunications (e.g., cell phone and landline service)
- Electric service for home consumption needs
- The financial infrastructure supporting banks and payment terminals

Compliance with the NERC CIP standards is critical for all stakeholders of the BES in the following jurisdictions:

- Eight provinces of Canada
- One state in Mexico
- The entire United States of America

Stakeholders of the BES include:

- Owners of assets on the BES such as:
    - Investors owning utilities
    - Merchants generating electricity
    - State or municipality entities
- Users or consumers of utilities running on the BES
- Producers of utilities (e.g., gas, electricity, train manufacturers)
- Suppliers of utilities (e.g., private or publicly-held utility companies)

The process of developing the NERC Reliability Standards is driven by industry insights. As such, any stakeholder directly impacted by the reliability of the North American BES can participate in the development of standards.

With the help of a NERC CIP compliance partner, your organization will leverage the NERC CIP requirements summary to optimize security controls for your assets running on the North American utility grid.

NERC CIP Standards Summary: Active Requirements

There are currently 13 active NERC CIP standards guiding cybersecurity best practices for stakeholders on the North American BES. The NERC CIP standards summary provided below will help your organization secure all utility assets connected to IT networks from cybersecurity risks.

CIP-002-5.1a – Categorization of BES Cyber Systems

Under Standard CIP-002-5.1a, organizations are required to identify assets that must be secured from potential cybersecurity risks to prevent significant damage to the BES. Once identified, these assets must be categorized and secured with the appropriate controls to minimize disruptions to the reliability of the assets.

Assets may include:

- Control centers and their backups
- Transmission stations and substations
- Resources used to generate utilities
- Systems and facilities that support the restoration of systems
- Protection systems designed to maintain the reliability of BES operations

To safeguard assets, risk can be categorized as high, medium, or low, depending on the type of asset and how critical it is to the reliability of the BES.

CIP-003-8 – Management of Security Controls

Standard CIP-003-8 outlines the responsibilities critical to safeguarding BES cyber systems from security risks that could compromise the reliability of the BES.

Stakeholders of BES assets are required to implement security controls focused on:

- Training personnel on appropriate security implementations
- Maintaining electronic security perimeters
- Enforcing physical security of assets
- Reporting security incidents and initiating appropriate response protocols
- Safeguarding sensitive information associated with BES assets
- Creating cybersecurity awareness

Documentation of all security controls will help streamline the safeguards implemented across assets on the BES.

CIP-004-6 – Training and Management of Security Personnel

According to Standard CIP-004-6, security awareness training must be conducted at least once each year to remind personnel of best practices for safeguarding assets on the BES.

The design of security awareness programs should account for controls related to:

- Proper implementation of cybersecurity policies
- Management of physical access controls
- Proper handling of sensitive BES system information
- Security risk management

Comprehensive background checks should also be conducted for all employees with direct access to systems operating BES assets to minimize security risks.

CIP-005-6 – Safeguarding Electronic Security Perimeters

Per Standard CIP-005-6, requirements for protecting BES assets via electronic security perimeters (ESPs) include:

- When assets are connected to networks via routable protocols, ESPs must be defined.
- External connectivity to assets must be routed through an electronic access point (EAP).
- All requests to access assets must be denied, except with access permissions.
- Dial-up connection requests must be authenticated.
- Malicious communications must be detected for all inbound or outbound communication.

Compliance with the ESP requirements is critical to mitigating risks of unauthorized access to BES assets and preventing disruptions in utility reliability.

CIP-006-6 – Physical Security of BES Cyber Systems

Per Standard CIP-006-6, the following physical security requirements must be implemented when complying with the NERC CIP:

- Physical access controls must be defined operationally and procedurally
- Guests physically accessing BES assets must be escorted at all times.
- If feasible, two or more physical access controls should be used.
- Unauthorized access should be monitored.
- Alarms should be issued where unauthorized physical access occurs.
- Physical access logs should be maintained to keep track of entry attempts.

Unauthorized physical access to BES assets can present serious risks to their reliability. Therefore, all physical access controls should be consistently optimized and monitored to ensure they function at the strictest acceptable levels..

CIP-007-6 – Management of Security Systems

Under Standard CIP-007-6, security systems safeguarding BES assets must be managed based on the following requirements:

- Logical ports with connections to assets must be disabled if they present security risks.
- Unnecessary physical or output ports must not be connected to BES assets, especially if they are from:
    - Network connections
    - Console commands
    - Removable media
- Security patches must be installed on all security systems.
- All installed security patches must be evaluated at least once every 35 calendar days.
- Any malicious code detected by security systems must be immediately removed.
- Security events must be logged for intelligence gathering.
- Security systems must generate alerts for critical security incidents.

The various types of security systems used to safeguard BES assets (e.g., electronic access control or monitoring systems (EACMS), physical access control systems (PACS)) must be kept up-to-date with industry standards to maximize their effectiveness.

CIP-008-6 – Incident Reporting and Response Planning

Standard CIP-008-6 stipulates the following requirements:

- Entities must implement one or more processes to identify and respond timely to security incidents.
- The roles and responsibilities of the security incident response personnel must be clearly defined.
- Procedures for handling security incidents must be documented.
- Incident response plans must be tested once every 15 months.
- Incident reports must be retained to optimize future responses.
- Following the testing of an incident response event, you should:
    - Document learnings
    - Update the existing response plan
    - Disseminate findings to the security team

When implemented correctly, incident response reporting and planning will improve your preparedness for any future incidents and help you manage them more effectively.

CIP-009-6 – Recovery Planning

The NERC CIP requirements for recovery planning under Standard CIP-009-6 include:

- When recovery plans are implemented, the conditions for their activation must be documented.
- The roles and responsibilities of incident responders must be clearly defined.
- The backup and storage of information necessary to recover the functionality of the BES must also be defined.
- Completion of backup processes must be verified, in case of failures.
- Data should be preserved, ensuring its preservation does not affect recovery.
- Recovery plans should be tested at least once every 15 calendar months.
- Following the testing of a recovery plan, any lessons learned must be documented.

The strength of NERC CIP recovery planning depends on the robustness of documentation processes.

CIP-010-3 – Configuration Change Management

When it comes to managing changes to configurations and conducting vulnerability assessments, Standard CIP-010-3 requires organizations to:

- Develop baseline change management configurations for security systems that contain:
    - Operating systems or firmware in instances where there isn't an independent operating system
    - Applications sourced commercially or via open source platforms
    - Custom software installations
    - Logical network accessible ports
    - Security patches
- Document changes that differ from baseline configurations, following authorization
- Update baseline configurations to reflect changes within 30 days of making the changes
- Verify that changes to baseline configurations meet the following requirements:
    - Security controls listed under CIP-005 and CIP-007 are implemented
    - The required security controls for baseline configurations are not affected
    - Results of the verification are documented

Changes to baseline configurations should also be:

- Tested within a test environment that ensures no adverse effects to baseline configurations or their relevant security controls
- Documented, after testing is complete, to show the differences between test and production environments

Furthermore, any software installed on security systems must be tested prior to deployment, and the source of the software should be verified. Similar to other NERC CIP controls, BES systems should be monitored every 35 calendar days to identify any risks to the configuration changes.

Vulnerability assessments are required every 15 calendar days and may be conducted as paper or active assessments. An active vulnerability assessment should be conducted whenever a new asset is added to the production environment, especially when baseline configuration models differ across assets.

CIP-011-2 – Protection of Information

Per Standard CIP-011-2, the information critical to operating BES systems must be protected during its storage, transit, and use.

Where assets are reused or disposed of, information must be protected, ensuring that system information cannot be retrieved from data storage media. In instances of asset disposal, the data storage media containing system information must be destroyed.

CIP-012-1 – Communications between Control Centers

Under Standard CIP-012-1, organizations must safeguard the communication of real-time assessment or monitoring data during its transmission between control centers.

Entities may implement a plan that includes:

- Mitigation of security risks with appropriate security protection
- Demonstration of compliance with secure data transmission protocols
- Clearly defined responsibilities for data transmission across control centers

Compliance with CIP-012-1 will minimize data transmission risks that could compromise BES assets at control centers and beyond.

CIP-013-1 – Management of Supply Chain Risk

To manage risks to the supply chain of the BES, Standard CIP-013-1 requires entities to develop a supply chain risk management plan for medium and high-impact BES assets.

The supply chain risk management plan should include:

- Processes for planning BES cyber system procurement and assessment of security risks to BES assets
- Processes to manage communication with vendors regarding:
    - Notification about vendor-identified risks to BES cyber systems
    - Coordinating responses to incidents identified by vendors that pose security risks to the BES assets
    - Restricting on-site or remote access to assets by vendor representatives
    - Disclosure of known vulnerabilities that present risks to BES systems
    - Verification of security patching and the integrity of software

Supply chain risk management must also be documented to ensure that risks are fully managed across all procured BES cyber systems.

CIP-014-3 – Physical Security

The physical security requirements listed under Standard CIP-014-3 include:

- Risk assessments must be conducted at transmission stations and substations at the following intervals:
    - Once every 30 calendar months where a risk assessment has been conducted and risks to substations or stations could compromise their reliability
    - Once every 60 calendar months where a risk assessment has not been previously conducted

Risk assessments must be verified by unaffiliated third parties such as:

- Registered planning, transmission, or reliability coordinators
- Entities with experience in transmission planning or analysis

Following risk assessments, entities must make recommended changes within 60 calendar days of the verification. Documentation is critical to ensuring that each step of the risk assessment process meets your security and compliance needs.