NERC Standards: NERC CIP Explained for the Energy Sector

The North American Electric Reliability Corporation (NERC) mandate encompasses technical and procedural requirements to guarantee the safety, security, and reliability of power transmission and generation. Compliance with NERC's standards is crucial for effective policy administration, cyber and physical access control, personnel management, and training.

Within the broader NERC standards, a subset of standards known as the NERC Critical Infrastructure Protection (CIP) standards are dedicated to regulating, enforcing, monitoring, and managing the security of the Bulk Electric System (BES) in North America. The NERC CIP standards specifically address the cybersecurity aspects of the BES and provide a framework to identify and secure critical assets that are essential for maintaining the efficient and reliable supply of electricity in North America.

This info guide aims to explain the significance of each of the 14 NERC CIP standards, their background, and their importance for the energy sector.

Why is NERC CIP Important?

The NERC CIP standards play a crucial role in safeguarding the reliability and security of the North American power grid. A successful cyberattack on the power grid could have catastrophic consequences, including widespread power outages, social disorder, economic disruption, and even loss of life. Therefore, compliance with these standards is of utmost importance to mitigate the risks associated with cyber threats.

Overview of NERC CIP Standards

The NERC CIP standards consist of a set of 47 requirements and 100 sub-requirements that encompass various aspects of cybersecurity in the BES. Let's delve into some of the key NERC CIP standards.

1. **NERC CIP-001: Sabotage Reporting**
   This standard requires the reporting of any incidents or suspicions of sabotage to relevant agencies, systems, regulatory bodies, or private entities. Infrastructure owners must have a system in place to investigate potential insider threats or sabotage situations and ensure employees are educated about the reporting process.

2. **NERC CIP-002: Critical Cyber Asset Identification**
   CIP-002 is possibly one of the most important standards because it focuses on the identification and documentation of critical cyber assets. By identifying these assets, organizations can assess the potential impact level, evaluate vulnerabilities, and implement necessary communication and risk management measures.

3. **NERC CIP-003: Security Management Controls**
   The NERC CIP-003 standard mandates the implementation of minimum-security management controls to protect critical cyber assets. These controls must include emergency procedures, documentation of changes, well-defined cybersecurity policies, designated personnel, annual reviews, and accessible information protection policies.

NERC CIP STANDARDS	
Standard	**Topic**
CIP- 001	Sabotage Repor ng
CIP- 002	Cri cal Cyber Asset Iden fica on
CIP- 003	Security Management Controls
CIP- 004	Personnel and Training
CIP- 005	Electronic Security Perimeters
CIP- 006	Physical Security of Cri cal Cyber Assets
CIP- 007	Systems Security Management
CIP- 008	Incident Repor ng and Response Planning
CIP- 009	Recovery Plans for Cri cal Cyber Assets
CIP- 010	Configura on Change Management
CIP- 011	Informa on Protec on
CIP- 012	Protect Real- me Data Integrity
CIP- 013	Supply Chain Risk Management
CIP- 014	Physical Security

4. **NERC CIP-004: Personnel and Training**

   NERC CIP-004 requires all personnel, as well as any person within the physical security perimeter, to receive a specific security designation. These security designations are vital to the auditing process and aid in an investigation after a breach. Thorough background checks should be completed on all potential personnel, contractors, and service vendors. In addition, all personnel are required to receive awareness training and additional training as needed or required.

5. **NERC CIP-005: Electronic Security Perimeters**

   This standard focuses on protecting critical cyber assets through the implementation of firewalls and securing all access points. Annual cyber vulnerability assessments are required to ensure continuous monitoring and improvement of the system's security.

6. **NERC CIP-006: Physical Security of Critical Cyber Assets**

   CIP-006 is intended to aid the entity in working to create and maintain a physical security plan. The physical security plan must undergo an annual review and address procedures for the following (at minimum):

   - Identify all access points through the physical security perimeter and measures to control entry to those access points.
   - Provide physical access to the perimeter(s), including keycards, computer access, manual logging, and biometrics.
   - Ensure proper use of physical access controls, including visitor pass management, responding to lost cards, and preventing unauthorized use of physical access controls.
   - Escort unauthorized personnel within the physical security perimeter.
   - Review access authorization requests and revocation authorization access.
   - Update the physical security plan within 90 calendar days of any physical security system changes, including reconfiguration, redesign, or updates.

7. **NERC CIP-007: Systems Security Management**
   NERC CIP-007 emphasizes the testing, review, and maintenance of security management systems. Monitoring passwords, antivirus software, malware detection programs, firmware, and IP ports or services is crucial to ensure the ongoing security of the system.
8. **NERC CIP-008: Incident Reporting and Response Planning**
   This standard requires the development and maintenance of a cybersecurity incident response plan. It should include procedures for classifying events, communication chains, employee roles in case of a breach, annual updates, and reporting information to relevant authorities.
9. **NERC CIP-009: Recovery Plans for Critical Cyber Assets**
   Entities must annually review and update a disaster recovery plan, defining responsibilities, backup systems procedures, and conducting disaster recovery plan exercises.
10. **NERC CIP-010: Configuration Change Management**
    NERC indicates that mandate CIP-010 is one of the most important. This standard aims to limit unauthorized access and changes to authorized users that could affect the BES operations. Configuration change management includes documenting and reporting changes to operating systems, software, patches, and application software.
11. **NERC CIP-011: Information Protection**
    Standard CIP-011-1 mandates that responsible entities implement protection controls to safeguard BES Cyber System Information. This standard is an integral part of a suite of CIP Standards focused on cybersecurity. It focuses on the protection of sensitive information associated with critical assets. It requires the implementation of measures like encryption, access controls, and secure storage to safeguard sensitive information from unauthorized access or disclosure.
12. **NERC CIP-012-1: Protect Real-Time Data Integrity**
    This standard ensures the protection of real-time assessment and monitoring data transmitted between bulk electric system Control Centers, supporting situational awareness and reliable operations.
13. **NERC CIP-013: Supply Chain Risk Management**
    NERC CIP-013-1 aims to mitigate cybersecurity risks to the reliable operation of the BES by implementing supply chain security controls for BES Cyber Systems. It mandates responsible entities to develop documented supply chain cybersecurity risk management practices.
14. **NERC CIP-014: Physical Security**
    The NERC CIP-014 standard focuses on enhancing physical security measures to protect critical assets. It requires the identification and protection of critical substations and control centers against physical threats, including sabotage, vandalism, and terrorist attacks.

Importance of NERC CIP Standards for the Energy Sector

- **Enhancing Grid Resilience:** NERC CIP standards provide a systematic approach to cybersecurity, ensuring the resilience of the energy grid against cyber threats and attacks.

- **Regulatory Compliance:** Compliance with NERC CIP standards is mandatory for entities operating within the North American bulk power system, ensuring a consistent and high level of cybersecurity across the sector.
- **Mitigating Risks:** By implementing the NERC CIP standards, organizations can identify, assess, and mitigate cybersecurity risks, reducing the potential for operational disruptions and financial losses.
- **Protection of Critical Assets:** The standards enable organizations to identify and prioritize critical assets, implement appropriate security controls, and safeguard them against cyber and physical threats.
- **Incident Response and Recovery:** NERC CIP standards emphasize the importance of incident response planning, facilitating a timely and coordinated response to cybersecurity incidents, and minimizing their impact.
- **Collaboration and Information Sharing:** The standards foster collaboration and information sharing among entities, enabling collective efforts to address emerging threats, vulnerabilities, and best practices.

(Also see Certrec's white paper: NERC CIP: The Importance of Critical Infrastructure Protection in the Energy Sector)

- **Bonus Learning**

  The most violated NERC CIP standard is CIP-007-6 (Cybersecurity — Systems Security Management). It has received the highest number of violations, with 108 instances, nearly twice as many as the next most-cited standard, CIP-010-4 (Cybersecurity — Configuration Change Management and Vulnerability Assessments).

Next Steps

To assess your organization's compliance with NERC CIP standards, you can take advantage of Certrec's NERC CIP Health Check, which offers a free assessment. Additionally, Certrec provides comprehensive and targeted NERC CIP gap analyses to help you identify and address any compliance gaps in your organization. For more information, contact Certrec at NERCExperts@certrec.com.

About Certrec:

Certrec is a leading provider of regulatory compliance solutions for the energy industry. Our SaaS and consulting services have helped hundreds of power-generating facilities manage their regulatory compliance and reduce their risks across nuclear, fossil, solar, wind, and other power plants. Certrec has helped more than 120 generating facilities establish and maintain NERC compliance, and we manage the entire NERC compliance program for 60+ registered sites in the US and Canada that trust us to decrease their regulatory and reputational risk. Certrec is ISO/IEC 27001:2022 certified and has successfully completed a SOC 2 Type 2 examination, resulting in independent verification of the standards of security, availability, reliability, and trusted services that we provide.

Contact us
6500 West Freeway, Suite 400
Fort Worth, TX 76116
817-738-7661
www.certrec.com

Legal Disclaimer