Life Is On | Schneider Electric

NERC CIP compliance for the power generation industry

Developing a comprehensive program to comply with NERC CIP* cybersecurity requirements

Solution at a glance

The Schneider Electric cybersecurity team ensures you meet all relevant NERC CIP standards for cybersecurity compliance. Our methodology is:

- Extremely adaptive
- Vendor-agnostic
- Network-independent
- Industry-relevant
- Lifecycle-based

Comprehensive cybersecurity

While the growth of digital network technology has ushered in a generation of increased reliability, improved safety, and reduced downtime, these same networks are now under regulatory review via the expansive NERC CIP standards for cybersecurity compliance.

Schneider Electric has the resources, expertise, and experience to help you develop and execute comprehensive programs to ensure compliance.

*North American Electric Reliability Corporation, Critical Infrastructure Protection

NERC CIP compliance for the power generation industry

Developing a comprehensive program to comply with NERC CIP cybersecurity requirements

Developing a comprehensive program takes time and a unique approach for each facility.

Achieving NERC CIP compliance involves the following:

- Identifying vulnerable assets
- Listing the gaps
- Developing a remediation plan
- Executing the implementation
- Monitoring the network
- Maintaining documentation

Because a facility's already thin workforce may not have the skills or knowledge necessary in developing and executing such a program, the Schneider Electric cybersecurity team can partner with clients to ensure NERC CIP compliance.

NERC CIP regulations

Each of the NERC CIP standards addresses a specific tenet of cybersecurity compliance regulations. The goal of NERC CIP is to establish a methodology and process for the protection of all digital assets with a compliant routable protocol.

Standard	Description
CIP-002	BES Cyber System Categorization
CIP-003	Security Management Controls
CIP-004	Personnel & Training
CIP-005	Electronic Security
CIP-006	Physical Security of BES Cyber Systems
CIP-007	Systems Security Management
CIP-008	Incident Reporting & Response Planning
CIP-009	Recovery Plans for BES Cyber Systems
CIP-010	Configuration Change Management and Vulnerability Assessments
CIP-011	Information Protection
CIP-014	Physical Security

Although the CIP standards are numerous and can appear onerous, these same standards can look less burdensome when viewed in their logical groupings:

Electronic security (CIP-002, 003, 005, 007, 009, 010, 011)

- Maintain an inventory of all electronics that are either part of the critical assets list or necessary to the operation of critical assets.
- Protect access to these critical cyber assets on a need-to-know basis.
- Create an electronic security perimeter that prevents unauthorized users from accessing any critical cyber asset, whether they are outside or inside the corporate network.
- Ensure that all cyber assets are secure via user account management, equipment, password management, and secure networking policies.
- Implement and test a Critical Cyber Asset recovery plan.

NERC CIP compliance for the power generation industry

Developing a comprehensive program to comply with NERC CIP cybersecurity requirements

Physical security (CIP-006, 014)
- Ensure that there is a physical security perimeter around all critical cyber assets.
- Identify and control physical access points to Critical Cyber Assets.
- Maintain an access log for all Critical Cyber Assets, via keycards, video, or manual log.

Personnel security (CIP-004)
- Investigate each person who accesses Critical Cyber Assets, including utilities personnel, contract workers, and vendors, to assess the risk that he or she poses to security.

Training and awareness (CIP-004)
- Train everyone who has access to Critical Cyber Assets, including utilities personnel, contract workers, and vendors, in cybersecurity

Incident reporting and response planning (CIP-008)
- All NERC CIP standards
- Recording of all cybersecurity incidents
- Internal computer incident response team (CIRT)
- Reporting to electricity sector information sharing and analysis (ES ISAC)

Recovery plans (CIP-009)
- Mandatory recovery plans
- Backup strategies
- Data restoration strategies
- Spare parts and equipment

Audits and documentation requirements for all CIP standards
- It is mandatory to document and review all procedures and policies yearly.
- NERC will audit compliance on all standards on a schedule provided by the organization.

At the core of these standards is identifying all bulk electrical system (BES) Cyber Assets and maintaining logs and records to help ensure that these assets are secure. This is not a one-time event, but a program that will last the life of the system — changing as new elements are added, old ones are removed, and any updates occur.

NERC CIP compliance

The Schneider Electric cybersecurity team's approach to compliance is consultative. Our consultants meet with you and your team to properly scope out an engagement. We then follow this initial meeting with a workshop, such as our electronic security perimeter (ESP) workshop. The ESP workshop is a collaborative meeting where many of the issues surrounding BES Cyber Asset identification (CIP-002) are addressed. The next step is an assessment as defined by the ESP workshop. Once all gaps are identified, we will propose an approach to best address your site requirements. Some of the services offered by Schneider Electric include:

- **Access controls —** firewalls, intrusion detection systems, secure zones configuration, design, and documentation
- **Logging —** event logging and alerting
- **Patching —** software solution geared to control network requirements
- **Performance monitoring and alerting —** solutions for tracking network and cyber asset performance data with historical reporting capabilities
- **Secure remote access —** solutions and services for deploying secure remote access (Hyper V technology)
- **GAP analysis —** work with customers to identify shortfalls or starting points for compliance programs
- **Vulnerability assessments —** identify attack vectors and the associated risks

NERC CIP compliance for the power generation industry

Developing a comprehensive program to comply with NERC CIP cybersecurity requirements

- **Hardening, patching services, AV solutions, system backups, and solution documentation**
- **Policy and procedure creation and updates** — policies and procedures written to meet control network requirements

The above methodology supports a NERC CIP-compliant network.

Cyber-compliant network

- Access controls for multiple secure zones
- Centralized:
  - Backups
  - Antivirus management
  - Patch management
  - Event management
- Network performance monitoring
- Historical data reporting
- Security event data reporting
- Active directory access controls
- Secure remote access relay server

Benefits

Our methodology is extremely adaptive and flexible, with a number of benefits that make it ideal for cyber compliance programs.

- Vendor-agnostic
- Network-independent
- Industry-relevant
- Lifecycle methodology-based
- 24/7 managed secure services

NERC CIP compliance for the power generation industry

Developing a comprehensive program to comply with NERC CIP cybersecurity requirements

Here is how Schneider Electric can make your facility NERC CIP cybersecurity compliant:

Standard	Description	Schneider Electric Solution
CIP-002	**BES Cyber System Categorization**	
CIP-002 R1	Review/Approve BES Cyber System Lists every 15 months	ESP Assessment
CIP-002-R2	Critical Asset (CA) Identification Methodology	ESP Workshop
CIP-003	**Security Management Controls**	
CIP-003 R1	Cybersecurity Policy	Policies and Procedures
CIP-003 R2	Leadership	
CIP-003 R3	Exceptions	Consulting Engagement
CIP-003 R4	Information Protection	Consulting Engagement
CIP-003 R5	Access Control	Consulting Engagement
CIP-003 R6	Change Control & Configuration Management	Policies and Procedures
CIP-004	**Personnel & Training**	
CIP-004 R1	Awareness	*Consulting Engagement
CIP-004 R2	Training	*Consulting Engagement
CIP-004 R3	Personnel Risk Assessment	*Consulting Engagement
CIP-004 R4	Access	Policies and Procedures
CIP-005	**Electronic Security**	
CIP-005 R1	Electronic Security Perimeter (ESP)	Solutions
CIP-005 R2	Electronic Access Controls	Solutions
CIP-005 R3	Monitoring Electronic Access	Solutions
CIP-005 R4	Cyber Vulnerability Assessment	Solutions
CIP-005 R5	Documentation Review & Maintenance	Solutions
CIP-006	**Physical Security of BES Cyber Systems**	
CIP-006 R1	Physical Security Plan	**Consulting Engagement
CIP-006 R2	Physical Access Controls	**Consulting Engagement
CIP-006 R3	Monitoring Physical Access	**Consulting Engagement
CIP-006 R4	Logging Physical Access	**Consulting Engagement
CIP-006 R5	Access Log Retention	**Consulting Engagement
CIP-006 R6	Maintenance and Testing	**Consulting Engagement
CIP-007	**Systems Security Management**	
CIP-007 R1	Test Procedures	Policies and Procedures
CIP-007 R2	Ports and Services	Solutions
CIP-007 R3	Security Patch Management	Solutions
CIP-007 R4	Malicious Software Prevention	Solutions
CIP-007 R5	Account Management	Solutions
CIP-007 R6	Security Status Monitoring	Solutions
CIP-007 R7	Disposal or Redeployment	Policies and Procedures
CIP-007 R8	Cyber Vulnerability Assessment	Solutions
CIP-007 R9	Documentation Review & Maintenance	Policies and Procedures

* Custom programs are available **Reporting and electronic access

NERC CIP compliance for the power generation industry

Developing a comprehensive program to comply with NERC CIP cybersecurity requirements

Here is how Schneider Electric can make your facility NERC CIP cyber security compliant (continued):

Standard	Description	Schneider Electric Solution
CIP-008	**Incident Reporting & Response Planning**	
CIP-008 R1	Cybersecurity Incident Response Plan	Policies and Procedures
CIP-008 R2	Cybersecurity Incident Documentation	Policies and Procedures
CIP-009	**Recovery Plans for BES Cyber Systems**	
CIP-009 R1	Recovery Plan	Policies and Procedures
CIP-009 R2	Recovery Exercises	Solutions
CIP-009 R3	Change Control	Policies and Procedures
CIP-009 R4	Backup and Restore	Policies and Procedures
CIP-009 R5	Testing Backup Media	Solutions
CIP-010	**Configuration Change Management and Vulnerability Assessments**	
CIP-010 R1	Configuration Change Management Process	Policies and Procedures
CIP-010 R2	Configuration Monitoring	Solutions
CIP-010 R3	Vulnerability Assessments	Solutions
CIP-011	**Information Protection**	
CIP-011 R1	Information Protection Process	Policies and Procedures
CIP-011 R2	BES Cyber Asset Reuse and Disposal	Policies and Procedures
CIP-014	**Physical Security**	
CIP-014 R1	Risk Assessment	Solutions
CIP-014 R2	Verify Risk Assessment	Solutions
CIP-014 R3	Risk Identification/Notification	Solutions
CIP-014 R4	Risk Evaluation	Solutions
CIP-014 R5	Physical Security Plan	Policies and Procedures
CIP-014 R6	Physical Security Plan Review and Evaluation	Policies and Procedures

Schneider Electric

70 Mechanic Street
Foxborough, MA 02035 USA
+1 877 342 5173

schneider-electric.com/processautomation

Life Is On Schneider Electric