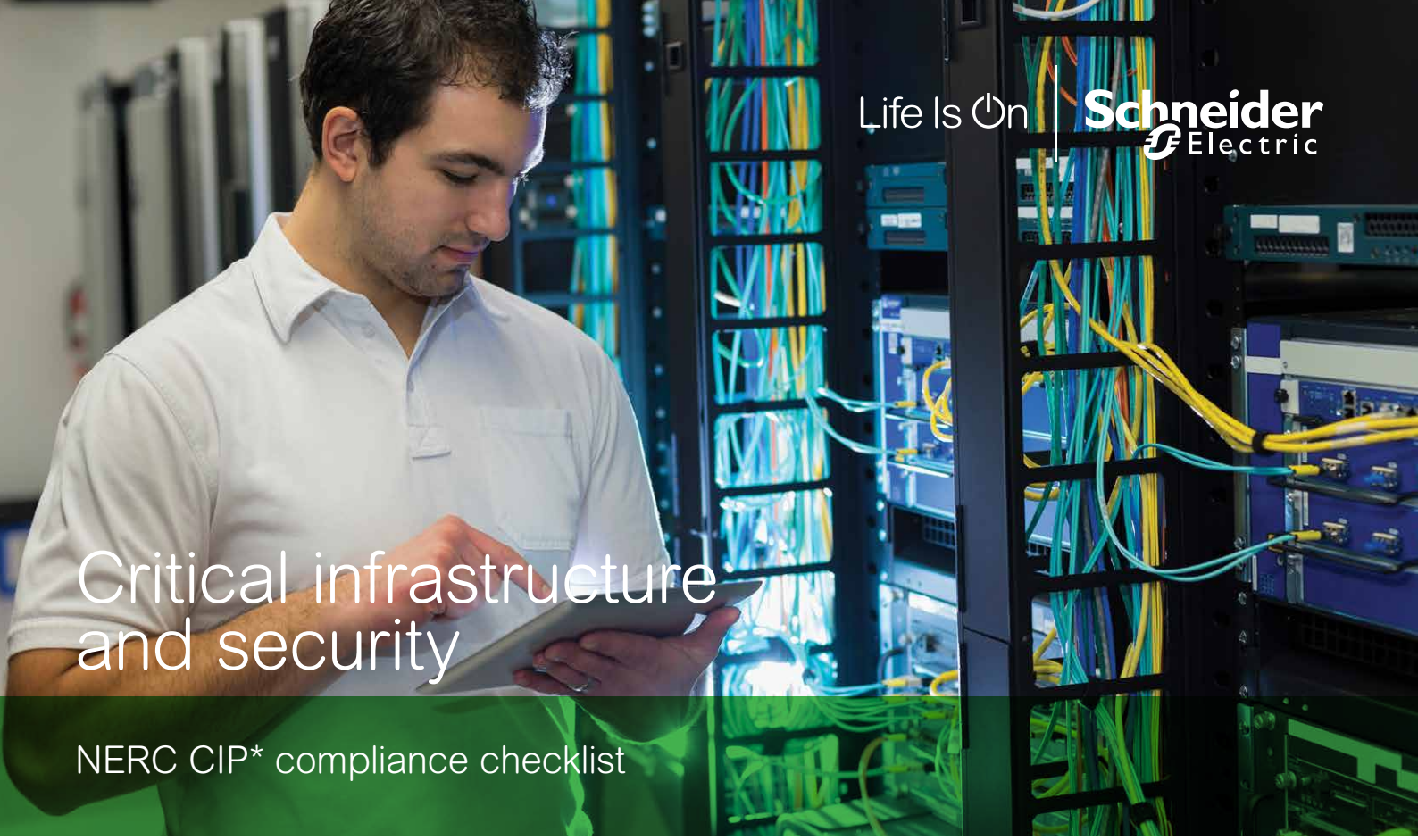

Life Is On | Schneider Electric

# Critical infrastructure and security

## NERC CIP* compliance checklist

### Service at a glance

As more control systems continue to migrate from analog to digital controllers, so does dependency on TCP/IP networks and the accompanying routable protocols. This brings these networks under the regulatory review of the expansive NERC CIP standards for cybersecurity compliance.

Schneider Electric's cybersecurity team possesses strong technical knowledge, industry experience, and cybersecurity trained personnel to assist companies in making their networks NERC CIP-compliant.

### Securing critical infrastructure

The mission of the North American Reliability Corporation (NERC) is to ensure the reliability of North America's bulk power system. NERC is certified by the U.S. Federal Energy Regulatory Commission (FERC) to establish and enforce reliability standards. NERC Critical Infrastructure Protection (CIP), or NERC CIP, is a set of regulatory standards adopted in 2006. These standards specify the minimum requirements to support the reliability of the electrical system. All organizations involved risk significant fines and penalties for lack of compliance, ranging as high as $1 million per day.

*North American Electric Reliability Corporation, Critical Infrastructure Protection

# Critical infrastructure and security

## NERC CIP compliance checklist

Merely deploying simple firewalls, secure servers, and antivirus software is not sufficient to become CIP-compliant. The NERC Standards CIP-002 through CIP-014 provide for a comprehensive cybersecurity framework. NERC CIP compliance encompasses electrical, physical, and personnel security as well as training and awareness.

- Electronic Security (CIP-002, CIP-003, CIP-005, CIP-007, CIP-008, CIP-009, CIP-010, CIP-011)
- Physical security (CIP-006, CIP-014)
- Personnel and training (CIP-004)

Schneider Electric's cybersecurity specialists augment plant staff in assessing, designing, implementing, and planning a comprehensive NERC CIP compliance program. We offer a comprehensive cybersecurity-compliant solution portfolio that addresses security assessment, security architecture and policy deployment, security implementation, and security management.

### NERC CIP security-compliant portfolio

Schneider Electric has the technical knowledge, industry experience, and cybersecurity-trained personnel to assist any company in making any network NERC CIP-compliant.

**Hardware independence:** Cybersecurity-compliant solutions work on any vendor's control systems and any type of security technology.

**Regulation knowledge:** We have a thorough understanding of NERC CIP regulations and participation in a number of industry and government groups.

**Technology knowledge:** Our team is versed in the latest security policies, procedures, and technologies for intrusion detection and prevention, firewalls, and DCS.

**Proven methodology:** Security-compliant portfolio is based on a lifecycle management methodology, ensuring compliance at any stage of network deployment.

# Critical infrastructure and security

## NERC CIP compliance checklist

This table is a reference to the NERC CIP standards and their corresponding reference numbers.

| Network Security | | |
|---|---|---|
| CIP-002 | Basic electrical system (BES) Cyber System Categorization | • BES Cyber Asset Classification (R1)<br>• Review/approve BES Cyber System Lists every 15 months (R2) |
| CIP-003 | Security Management Controls | • Cyber Security Policy in Place (R1)<br>• Leadership Assignments (R2)<br>• Policy Exception Handling (R3)<br>• Information Protection (R4)<br>• Access Control (R5)<br>• Change Control/Configuration Management (R6) |
| CIP-005 | Electronic Security Perimeters | • Establish Electronic Security Perimeter (R1)<br>• Electronic Access Controls (R2)<br>• Monitoring Electronic Access (R3)<br>• Cyber Vulnerability Assessment (R4)<br>• Documentation Review & Maintenance (R5) |
| CIP-007 | Systems Security Management | • Test Procedures (R1)<br>• Ports & Services (R2)<br>• Security Patch Management (R3)<br>• Malicious Software Prevention (R4)<br>• Account Management (R5)<br>• Security Status Monitoring (R6)<br>• Disposal or Redeployment (R7)<br>• Cyber Vulnerability Assessment (R8)<br>• Documentation Review & Maintenance (R9) |
| CIP-008 | Incident Reporting and Response Planning | • Cyber Security Incident Response Plan (R1)<br>• Incident Documentation (R2) |
| CIP-009 | Recovery Plans for BES Cyber Systems | • Recovery Plans (R1)<br>• Exercises (R2)<br>• Change Control (R3)<br>• Backup & Restore (R4)<br>• Testing Backup (R5) |
| CIP-010 | Configuration Change Management and Vulnerability Assessments | • Configuration Change Management Process (R1)<br>• Configuration Monitoring (R2)<br>• Vulnerability Assessments (R3) |
| CIP-011 | Information Protection | • Information Protection Process (R1)<br>• BES Cyber Asset Reuse and Disposal (R2) |

# Critical infrastructure and security

## NERC CIP compliance checklist

This table is a reference to the NERC CIP standards and their corresponding reference numbers.

| | | |
|---|---|---|
| **Physical Security** | | |
| CIP-006 | Physical Security of BES Cyber Systems | • Physical Security Plan (R1)<br>• Physical Access Controls (R2)<br>• Monitor Physical Access (R3)<br>• Logging Physical Access (R4)<br>• Access Log Access (R5)<br>• Maintenance & Testing (R6) |
| CIP-014 | Physical Security | • Risk Assessment (R1)<br>• Verification of Risk Assessment (R2)<br>• Transmission Operator Controls (R3)<br>• Vulnerability Assessment (R4)<br>• Physical Security Plan (R5)<br>• Physical Security Plan Review (R6) |
| **Personnel Security** | | |
| CIP-004 | Personnel and Training | • Awareness (R1)<br>• Training (R2)<br>• Personnel Risk Assessment (R3)<br>• Access (R4) |

Schneider Electric

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

schneider-electric.com/processautomation

Life Is On Schneider Electric