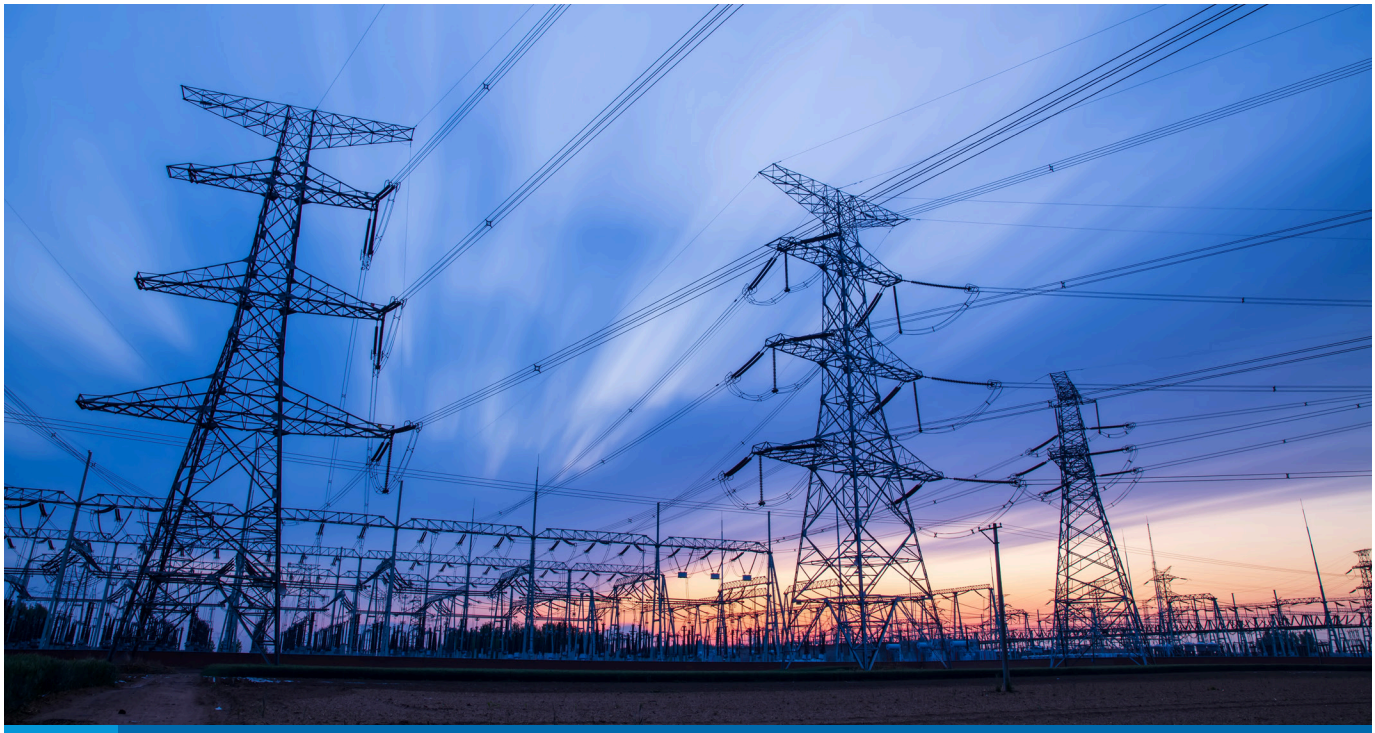
foxguard



Critical Infrastructure Protection:
Shifting the Burden

2285 Prospect Dr. NE
Christiansburg, VA 24073
877.446.4732
foxguardsolutions.com

Introduction

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), under the oversight of the Federal Energy Regulatory Commission (FERC), establishes compliance standards for the Bulk Electric System (BES). These standards place a heavy compliance burden on utilities who must ensure the uninterrupted generation, transmission, and distribution of electricity, safeguarding the grid from potential cyber risks.

Non-compliance with NERC CIP standards can result in significant penalties. In recent years multiple fines exceeding $1 million have highlighted the serious consequences of failing to meet these regulatory obligations.

Nearly two decades into the implementation of NERC CIP regulation, utilities within the BES have made significant efforts to understand the requirements and establish the necessary processes, controls and documentation to achieve and maintain compliance.

These measures are critical to protecting their assets and ensuring their contributions to the grid remain secure and reliable.

However, as NERC CIP standards continue to evolve, compliance has become an area requiring ongoing investment and attention. This evolving landscape increases the burden on utilities, particularly in areas like regular patching, vulnerability management and documentation. Even utilities that have diligently modernized their processes may still encounter challenges in maintaining compliance. Failure to comply can result in additional penalties and reputational harm within the industry.

Managing compliance across a large fleet of assets remains a complex task, requiring additional personnel, expertise and structured processes. By leveraging supplier-driven solutions to strengthen cyber security measures pre-deployment, utilities can better align with NERC CIP standards and maintain robust protections for the critical infrastructure that powers our communities.

Compliance with NERC CIP Reliability Standards is required by law to ensure the security and reliability of the bulk electric system (BES).

Cybersecurity — Systems Security Management

CIP-007-6

Purpose: To enhance system security by defining specific technical, operational and procedural requirements. These measures support the protection of Bulk Electric System (BES) cyber systems from compromises that could result in misoperation or instability of the BES.

Requirements

Ports and Services — where technically feasible, enable only the logical network-accessible ports deemed necessary by the responsible entity, including port ranges or services required for handling dynamic ports. If a device cannot disable or restrict logical ports, any open ports are considered necessary by default. Additionally, safeguard against the use of unnecessary physical input/output ports utilized for network connectivity, console commands or removable media.

Security Patch Management — a comprehensive patch management process is required to track, evaluate and install cyber security patches for applicable cyber assets. This process must also include identifying reliable sources that the responsible entity monitors for cyber security patch releases applicable to updateable cyber assets and for which a patching source exists.

Malicious Code Prevention — implement method(s) to deter, detect and prevent malicious code, and mitigate threats from any detected instances. For methods that rely on signatures or patterns, establish a process for updating these signatures or patterns, including their testing and installation.

Security Event Monitoring — log events at the BES cyber system level (per BES cyber system capability) or at the cyber asset level (per cyber asset capability) for identification of, and after-the-fact investigations of, cyber security incidents that include as a minimum, each of the following types of events:

- Detected successful login attempts
- Detected failed access attempts and failed login attempts
- Detected malicious code

— generate alerts for security events identified by the responsible entity as requiring notification: At a minimum, this includes the following event types, based on the capabilities of each cyber asset or BES cyber system:

- Detected malicious code
- Detected failure of event logging

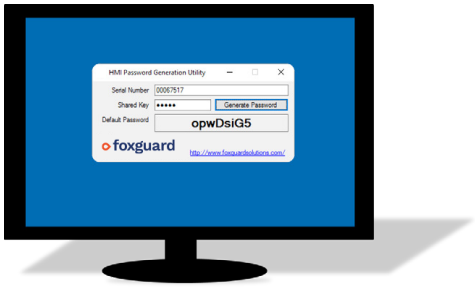
System Access Control — implement methods to enforce authentication for interactive user access, where technically feasible, including:

- Maintain an inventory of all known enabled default or generic account types, organized by system, group of systems, location, or system type.
- Identify individuals authorized to use shared accounts and ensure default passwords are changed in accordance with cyber asset capabilities.
- For password-only authentication, enforce password parameters for length and complexity as specified in the CIP-007-6 standard, either through technical measures or procedural controls.
- Where feasible, require password changes at least once every 15 calendar months, using technical or procedural methods.
- Additionally, where technically feasible:
  - Limit the number of unsuccessful authentication attempts, or
  - Generate alerts after a predefined threshold of unsuccessful attempts is reached.

Shifting the Burden

Now what if, before delivering their computing, networking and other programmable assets to the site, suppliers proactively addressed much of the work outlined in the CIP-007 standards? That would be a significant benefit to their utility customers. Shifting this burden would allow utility personnes.

This paper proposes the creation of an environment where—through adherence to internal cyber security controls—suppliers provide products that have been carefully and securely created, assembled, documented and shipped.

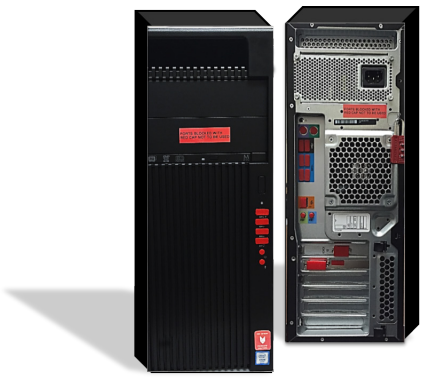


In power plant control rooms and substations, computers handle critical functions such as controls, SCADA and gateway operations. These systems could be the first to implement the supplier controls discussed above. Some companies have already integrated the necessary security measures into their supply chain and fulfillment processes. Below are examples of the potential outcomes for utilities, many of which align with the requirements set forth in NERC CIP-007.

The supplier facility would be secured with both physical and software controls. Only authorized personnel with the proper clearance and security privileges would have access to the equipment and information required for product assembly. To ensure NERC CIP compliance, a specific set of manufacturing steps would be followed during assembly, including:

Software

- The operating system and critical applications would be updated with the latest verified and tested security patches.
- A system audit would be conducted for all users, installed applications, security patches and ports and services.
- A vulnerability assessment would be performed using a third-party application such as Nessus.
- Final manufacturing checks would be performed including:
  - A full system scan using up-to-date and trusted anti-virus software
  - System diagnostics, final review for errors and associated documentation
  - Full system backup
  - Set up of a unique password for each system
  - Documentation of the final system shutdown



Hardware

To increase awareness of unauthorized access or misuse of physical ports, such as USB or Ethernet, install port blockers, attach warning labels, and secure chassis with combination locks to prevent access to internal components.

Documentation:

- Manufacturing steps that are critical to NERC CIP standards would be documented in two formats, electronic and hard copy.
- Hard copies would be placed in a unique binder for each system. This documentation would become the utility's baseline for NERC CIP audit preparation and for the ongoing maintenance of their compliance program.
- Custom cover page per platform
- Manufacturing quality signoff
- Hardware diagnostics report
- System overview
- List of users and groups
- List of installed software
- List of installed updates
- List of open ports
- List of service configuration
- Vulnerability Report
- Any additional information that might be specific to this implementation
- Training and User Guide (Per individual project requirements)

Packaging – tamper proof, branded, and serialized labels are used to ensure proper chain of custody.

Vendors of programmable assets subject to NERC CIP compliance requirements could complete these security processes before delivery to individual power plants or substation sites, supplying notable advantages to utilities. Customers could be confident that proper security controls where in place, while the responsibility for this work and the associated documentation shifts to the supply chain. This would allow the utility to focus on delivering safe and secure electricity.

How Foxguard Helps

Utilities have two primary options for improving compliance. One approach involves internal investments, though this can be costly, due to the need for new processes, specialized workforce expertise and advanced equipment for testing and validation. Alternatively, utilities can establish a high-level managerial strategy, assigning much of the compliance responsibility to their asset suppliers.

Foxguard supports this decentralized approach, helping utilities strengthen their security posture while ensuring compliance is baked into their processes from the start. By integrating patch management expertise with advanced vulnerability management tools, Foxguard shifts the burden of compliance from internal teams to a trusted partner.

Our extensive experience in delivering computing and cyber security solutions. Our expertise and solutions are directly aligned with NERC CIP requirements, helping utilities meet key compliance objectives, including:

1. **Asset Management** (CIP-002, CIP-003):
   Foxguard Discover enables utilities to establish and maintain a comprehensive inventory of critical assets, ensuring accurate classification and identification in line with NERC CIP standards.

2. **Patch Management** (CIP-007):
   Through solutions like the **Foxguard Patchintel** we ensure a simplified patching process by delivering timely updates for critical assets. This ensures that utilities stay compliant with the patching and vulnerability management requirements under CIP-007.

3. **Vulnerability Management** (CIP-008, CIP-009):
   Foxguard's Cyberwatch platform provides vulnerability assessments and actionable remediation strategies, reducing risks while maintaining compliance with incident response and recovery standards.

4. **Compliance Reporting** (CIP-010):
   By automating compliance documentation and providing a centralized platform for tracking activities, Foxguard reduces the administrative burden of meeting audit requirements.

These capabilities empower utilities to achieve continuous compliance while mitigating cyber security risks, reducing penalties and ensuring reliable operations. At Foxguard, our supplier-driven solutions enable utilities to preemptively address vulnerabilities and streamline compliance workflows. With over 800 customers across critical industries, including energy, nuclear, and transportation, Foxguard has proven success in helping organizations reduce risks, improve efficiencies and achieve regulatory compliance.

Key benefits of working with Foxguard include:

- Centralized patch management and vulnerability assessment
- Automated compliance reporting to streamline regulatory requirements
- A unified platform for managing IT and OT environments
- Proven compliance strategies developed in collaboration with the U.S. Department of Energy

By partnering with Foxguard, utilities can reduce the burden of compliance and cyber security, freeing their teams to focus on core operations. Our solutions align with the NIST Cybersecurity Framework and NERC CIP, ensuring your organization has a strong foundation to manage risks effectively.

We welcome the opportunity to consult with any utility customer interested in exploring these solutions further.

About Foxguard

Foxguard is your trusted advisor at every stage of your cyber security, custom computing and digitization journey. For critical infrastructure, we enhance operational safety, quality and uptime by strengthening your cyber security maturity. We meet your custom computing needs through end-to-end system integration of hardware and software solutions, ensuring a secure supply chain and effective lifecycle management. Foxguard is a wholly owned subsidiary of Framatome Inc. and a key part of the Framatome Cybersecurity Solutions line.

7k+	1.5M+	30k+	40+
Patchintel reports produced	Asset patching supports	Customer computing deployements	Years in business, since 1981

Contact:
877.446.4732
2285 Prospect Dr. NE
Christiansburg, VA 24073
foxguardsolutions.com