

ALCEA
ASSA ABLOY

protecting the U.S. power grid: NERC CIP Standards and Physical Security Solutions.

When threats are bigger, get tougher and smarter.

ALCEA
ASSA ABLOY



why NERC CIP Standards were created

The U.S. power grid is one of the most critical infrastructures supporting modern society, powering homes, businesses, and essential services. However, the grid has become increasingly vulnerable to both physical and cyber threats, including vandalism, terrorism, and cyber-attacks targeting operational technology. Recognizing the growing risks to this essential infrastructure, the Federal Energy Regulatory Commission (FERC) mandated the development of standards to protect the Bulk Electric System (BES) from potential compromise. The NERC Critical Infrastructure Protection (CIP) Standards were created to establish a structured, enforceable framework to mitigate vulnerabilities, enhance security, and ensure the reliability of the power grid in the face of evolving threats.

Key elements of NERC CIP Standards include:

- **Physical Security Perimeters (PSPs):** Defined physical borders around BES Cyber Systems and critical assets to control access and monitor potential threats.
- **Physical Access Control Systems (PACS):** Cyber assets used to control, alert, and log access to PSPs, ensuring only authorized personnel gain entry.
- **Two or More Access Controls:** High-impact BES Cyber Systems (HIBCS) require multiple layers of security controls to restrict access, such as dual-factor authentication or layered physical and electronic locks.
- **Audit and Traceability:** Utilities must log all access to PSPs and retain records for at least 90 days, ensuring accountability and enabling quick responses to breaches.
- **Maintenance and Testing:** Physical security systems and PACS must be tested every 24 months to ensure proper functionality, including granting access to authorized personnel, denying unauthorized access, and generating alarms.

The standards specify a systematic approach to securing critical infrastructure by requiring documented plans, monitoring systems, and response protocols. Compliance ensures that utilities can proactively manage physical access to BES Cyber Systems, reducing the risk of misoperation or instability in the power grid.

purpose and scope.

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards are critical to safeguarding the Bulk Electric System (BES), which powers the nation's economy and sustains daily life.

Directed by the Federal Energy Regulatory Commission (FERC), these standards aim to mitigate physical and cyber risks to critical infrastructure, requiring utilities to implement robust security programs.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- For the latest NERC standards and compliance news scan here:

(www.nerc.com/Pages/default.aspx)





meeting NERC CIP Standards with ALCEA locking solutions, powered by ABLOY

ALCEA's high-security locking systems and software solutions are designed to meet the stringent requirements of NERC CIP standards, providing robust, scalable, and adaptable solutions for securing critical infrastructure.

With hybrid mechanical and electromechanical options, these security and access systems ensure compliance while offering enhanced functionality and cost-efficiency.

1. High-security hybrid locking systems

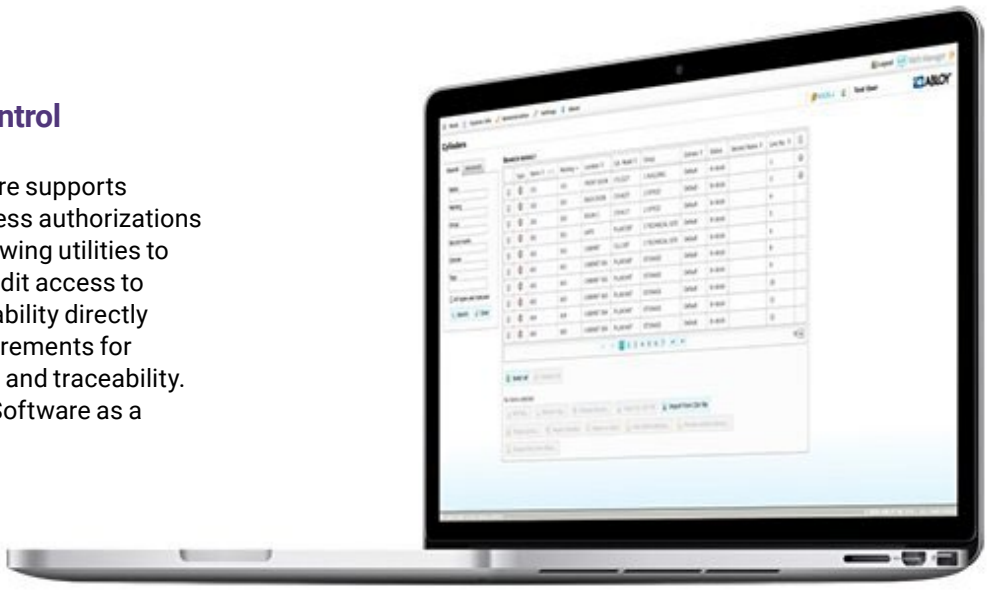
Mechanical security: ABLOY's rotating disc cylinder locks are more secure than pin-based locks and provide tamper-resistant physical protection, ensuring access is restricted to authorized personnel with precision key control.

Electromechanical CLIQ cylinders: These add an essential layer of cybersecurity, offering 100% control of all keys 100% of the time with remote access management, real-time tracking, and the ability to disable lost keys.

ABLOY High Security Padlocks: Challenging weather and extreme environmental conditions put stress on remote utility facilities. ABLOY padlocks provide extremely effective protection against forcing, picking and vandalism. Case hardened boron steel shackles offer exceptional durability and have successfully passed demanding corrosion tests.

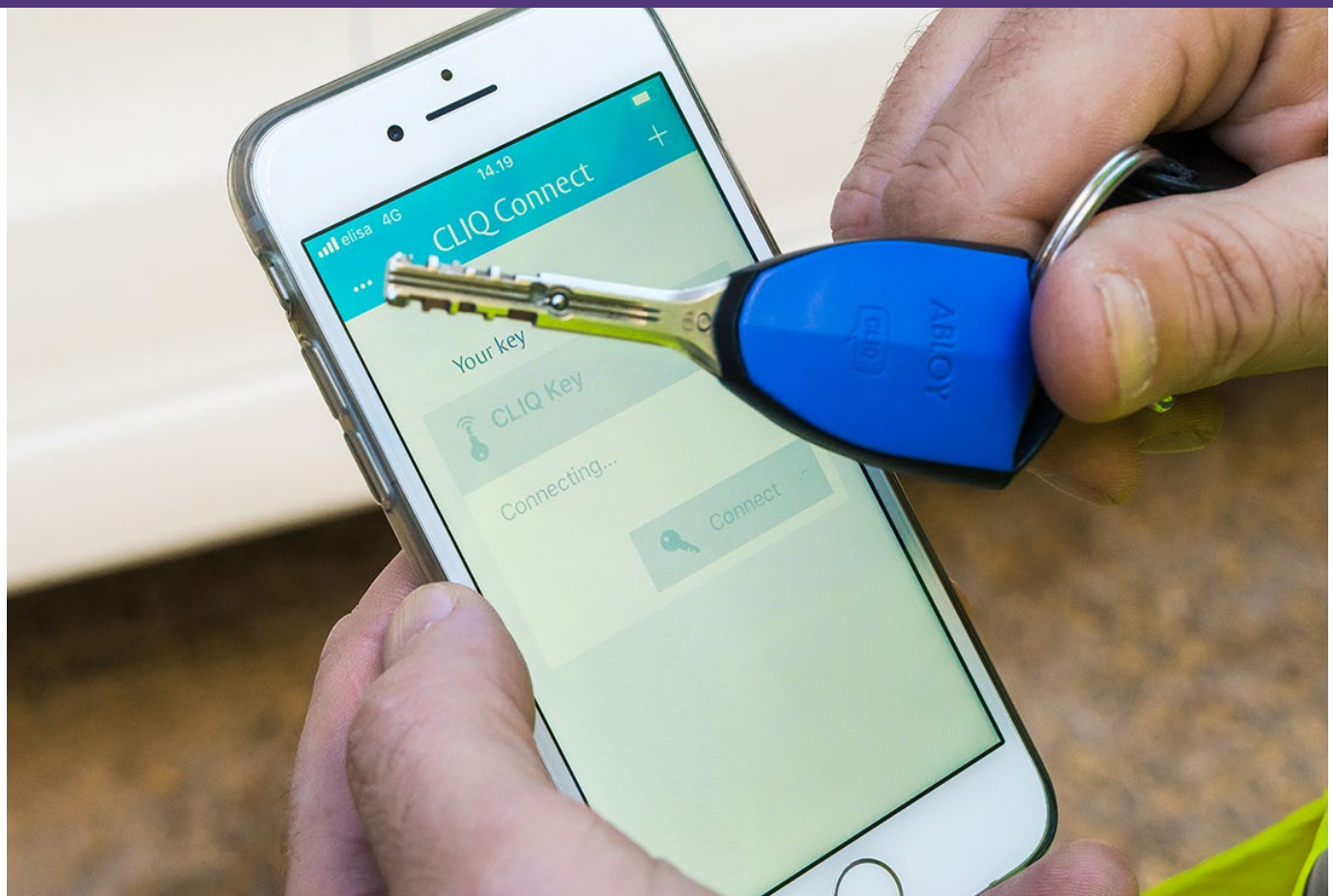
2. Advanced access control

Browser-based CLIQ software supports centralized control over access authorizations and keyholder activities, allowing utilities to manage permissions and audit access to PSPs dynamically. This capability directly aligns with NERC CIP's requirements for multi-factor access controls and traceability. Available as an in-house or Software as a Service option (SaaS).



3. Comprehensive monitoring and logging

ABLOY's solutions can integrate with PACS to enable real-time monitoring and alerting. Each access event is logged, supporting compliance with standards for access records and incident response. CLIQ makes it possible to update keys anywhere and anytime via iOS or Android device.



4. Cost-effective deployment

ABLOY's hybrid locking systems enable utilities to integrate both mechanical and electronic locks within the same infrastructure. This adaptable solution allows utilities to prioritize resources by deploying electronic locks in critical, high-priority areas while using mechanical locks in less sensitive locations.

By tailoring security measures to specific needs, utilities can reduce overall upgrade costs by up to 40% compared to implementing a fully electronic system—all while maintaining compliance and robust protection.



frequently asked questions about NERC CIP Standards

1. Are NERC CIP Standards mandatory?

Yes, compliance with NERC CIP Standards is mandatory for entities responsible for the Bulk Electric System (BES). These standards are enforced by the Federal Energy Regulatory Commission (FERC), which oversees adherence and has the authority to impose penalties for non-compliance.

2. How is compliance with NERC CIP Standards enforced?

FERC enforces compliance through audits conducted by the North American Electric Reliability Corporation (NERC) and its Regional Entities. Non-compliance can result in significant penalties, including monetary fines, reputational damage, and operational restrictions. Self-reporting non-compliance issues is encouraged and can mitigate penalties, but failing to disclose or address issues may result in harsher fines.

3. What are the consequences of non-compliance with NERC CIP Standards?

Penalties for non-compliance can include fines of up to $1 million per violation per day, operational restrictions, and damage to an organization's reputation. Ensuring compliance protects critical infrastructure and avoids the financial and operational risks associated with enforcement actions.

4. How often are NERC CIP Standards updated?

NERC CIP Standards are reviewed and updated periodically to address emerging threats and evolving technologies. The updates are driven by industry input, regulatory developments, and changes in cybersecurity and physical security landscapes. Entities are responsible for staying informed about updates and adjusting their compliance programs accordingly.

5. What is a Physical Security Perimeter (PSP)?

A PSP is the defined physical boundary surrounding BES Cyber Systems and related assets. It serves as the first line of defense by controlling and monitoring physical access, ensuring only authorized personnel can enter.

6. What is the role of a Physical Access Control System (PACS)?

A PACS controls, alerts, and logs access to PSPs. It plays a critical role in meeting NERC CIP requirements for real-time monitoring, incident response, and access traceability.

7. How do ALCEA locking solutions help utilities comply with NERC CIP?

ALCEA access management systems powered by ABLOY technology provide high-security mechanical and electromechanical solutions, including centralized access control, audit trail capabilities, and remote key management. These features align with NERC CIP's requirements for physical security and access accountability.

8. How do NERC CIP Standards address audit readiness?

NERC CIP requires utilities to maintain access logs, audit trails, and documentation for at least 90 days. These records demonstrate compliance during audits and provide evidence of security measures in place. Regular system testing and maintenance are also required to ensure preparedness for audits.

9. How do NERC CIP Standards impact small utility operators compared to large ones?

While the core requirements of NERC CIP Standards apply universally, the scale of implementation can vary significantly between small and large utility operators. Large utilities typically manage complex networks with numerous PSPs, requiring extensive resources to comply with logging, monitoring, and multi-layered access controls. Small utilities, on the other hand, often manage fewer assets but may face challenges due to limited budgets and personnel. Scalable solutions, such as ABLOY's hybrid locking systems, can help operators meet compliance requirements efficiently without overextending their resources.



case study

"We now know to whom keys are assigned, and if a key is lost, we can deactivate it or prevent unauthorized re-syncing. This system gives us a fresh start with clear audit trails."

— Director of Security for Large Midwest Utility.

large midwest utility meets NERC CIP Standards with ALCEA Solutions.

To develop a compliant physical security footprint, one large multi-state utility partnered with ALCEA and its security systems integrator to address new NERC CIP regulations. The utility adopted the ABLOY PROTEC² CLIQ® system, which combines high-security super weatherproof padlocks and an electromechanical access control system administered remotely.

Previously, key management at the utility was decentralized and undocumented. Keys were stored in drawers, distributed without oversight, and often lost or stolen. With all regional locations keyed alike, this posed significant security risks across their network.

strategic implementation for compliance.

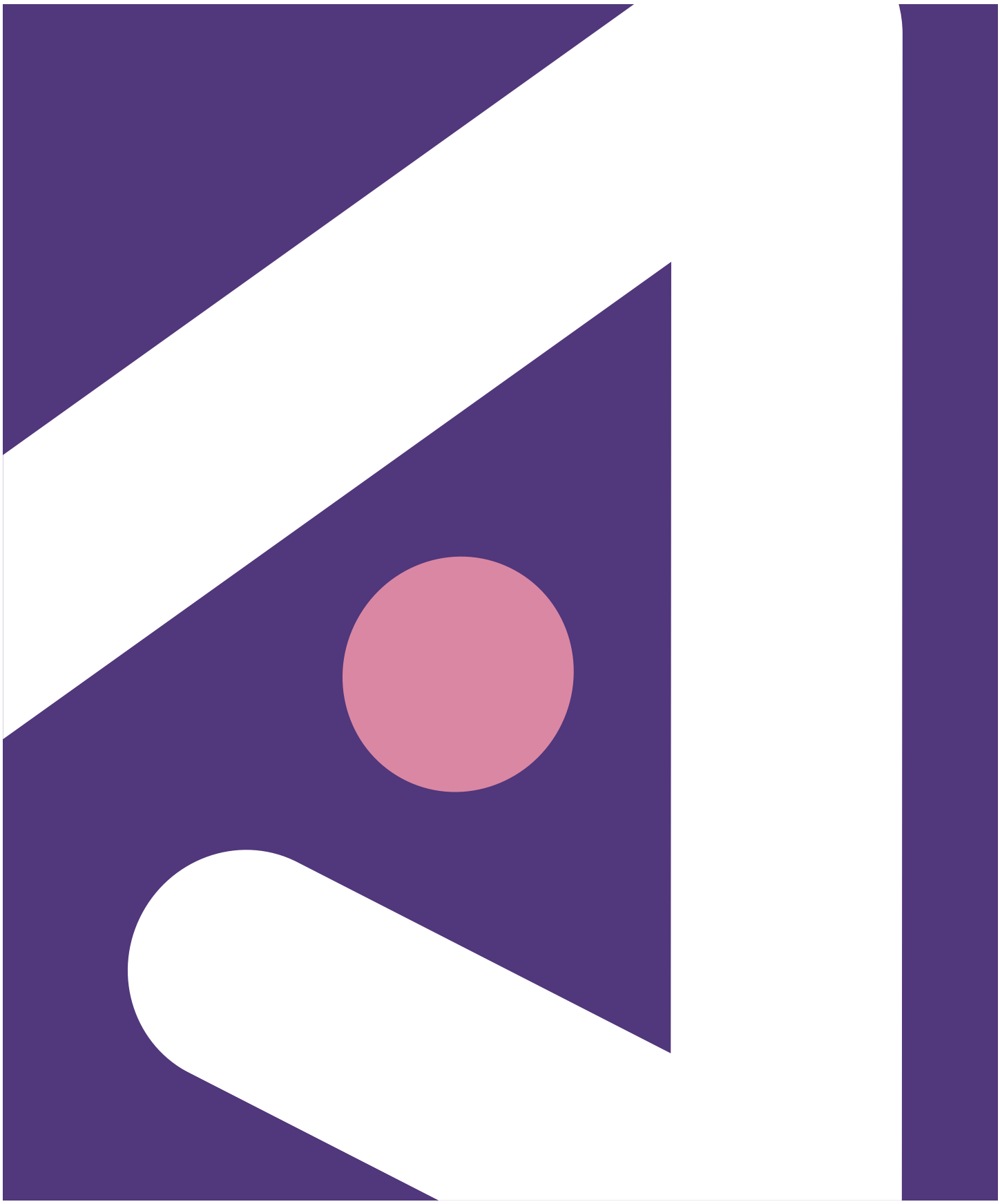
The utility, with the ALCEA team's assistance, created a plan to secure thousands of locking points across an eleven-state area. The PROTEC² CLIQ system enabled centralized access control with key tracking and remote deactivation capabilities. Lost or stolen keys could be quickly disabled, and keys that weren't re-synced within a set timeframe were automatically invalidated.

Security administrators could now issue keys systematically, track assignments, and generate audit trails to document access. This level of control and visibility helped the utility streamline operations while maintaining compliance with NERC CIP standards.

Results and Benefits

The utility standardized the PROTEC² CLIQ® system across all transmission and generation sites, ensuring a consistent and secure approach to physical security. With centralized control and robust logging capabilities, the company reduced risks associated with unauthorized access, improved efficiency, and ensured compliance with regulatory audits.





ALCEA specializes in protecting critical infrastructure globally, including energy, water, telecom, transportation, mining, oil, and gas. We provide comprehensive security solutions tailored to your unique needs, from access control and intrusion detection to key and video management. Our experienced specialists deliver customized, digitalized solutions that enhance efficiency, ensure compliance, and offer peace of mind.

© 2024 ALCEA/ASSA ABLOY AB. All rights reserved. This publication is for informational purposes only, without representation or warranty of any kind and the details provided herein are subject to change without advance notice.

alceaglobal.com

2025 copyright by ASSA ABLOY. All rights reserved. We reserve the right to make technical modifications. Version: ALCEA_WhitePaper_NERC CIP | 2025 | whitepaper