Keeping On Top of CIP Requirements Is Complicated. But Your NERC CIP Training Shouldn't Be.

Empower a secure workforce with SANS Security Awareness.

Working within heavily regulated industries, such as the North American Bulk Electric System (BES), maintaining and delivering effective cybersecurity training can be an ongoing struggle. With the complexities and unique vulnerabilities inherent to the BES, in is not uncommon for organizations to develop in-house training programs to meet compliance. But, maintaining CIP compliance in the face of constantly evolving threat vectors requires a level of cyber-expertise internal teams may not have readily available.

At SANS, our Security Awareness programs equip electrical utilities companies with a straightforward, up-to-date, and cost-effective training solution that does more than just meet CIP compliance – it actually better equips your teams to manage human risk.

Through short and engaging computer-based learning modules, all personnel that interact with critical systems can complete and record all required CIP training while learning how to apply concepts in real-world scenarios. The convenience of pre-built and auto-updated training frees up organizational resources typically tasked with NERC CIP training, resulting in huge savings in both time and costs.

NERC CIP Training Made Easy

Backed by SANS, the largest and most trusted source for information security training in the world, SANS Security Awareness NERC CIP Training is the most detailed, up-to-date curriculum addressing CIP-004 requirements on the market.

SANS Security Awareness NERC CIP Training delivers:

Unmatched Expertise

Leveraging input from an advisory board of the most well-known influencers in the space, our NERC CIP training is developed by industry practitioners and cognitive experts who ensure training meets the latest requirements, addresses the latest challenges, and makes a lasting impact.

Strategic Learning Approach

With so many requirements to meet, it's critical that learning modules do more than just teach concepts – they must train secure behaviors. All NERC CIP training is designed and continually assessed using adult learning science principles, ensuring curricula is relevant, engaging, and effective.

Built-for-Purpose Content

Each minutes-long NERC CIP training module reflects real-world working scenarios and links directly to relevant company policies, reducing learner fatigue and making compliance convenient. Plus, all content is developed in-house, maintaining the consistent, high-quality production value associated with SANS.

TRAIN ALL NERC CIP PERSONNEL WITH CONFIDENCE AND EASE.

SANS Security Awareness designs all NERC CIP learning modules with the unique needs of the electrical utilities industry in mind.

From system operators to IT departments to maintenance staff, literally anyone who interacts with a critical system is required to complete NERC CIP training. We make sure all our training is relevant and easy-to-understand, no matter where one falls in the organizational hierarchy. When industry standards change, we automatically update our training before new versions become enforceable, so businesses can rest assured that their organization is best positioned to stay in compliance.

SANS Security Awareness NERC CIP Training Modules

Our 12 computer-based learning modules are fully SCORM compliant and can be deployed on an existing learning management system, on the SANS-hosted Litmos learning platform.
Each module builds upon the last in the following order:

1. **Introduction:** An overview of the roles and responsibilities of FERC, NERC and NERC Regional Entities, as well as how NERC Registered entities must adhere to NERC CIP Reliability Standards.
2. **Terms and Definitions:** A brief walk-through of new and modified terms introduced in CIPv5 and CIPv6 standards.
3. **Operating Interconnected and Interdependent BES Cyber Systems:** A deep dive into common systems, networks and operational interdependence and how cybersecurity risks and events impact various components, including those associated with Transient Cyber Assets and Removable Media.
4. **Asset Identification and Requirement Applicability:** An analysis of the CIP-002 asset-identification process and the impact rating criteria approach included in Attachment 1, as well as the requirements, measures and itemized applicability approach of CIPv6 standards.
5. **NERC CIP Policy Requirements:** A breakdown of four key program policy areas required in CIPv6: Personnel and Training, System Security Management, Configuration Change Management and Vulnerability Assessments, and Declaring and Responding to CIP Exceptional Circumstances.
6. **Electronic Access Controls:** A review of CIP-005 approaches for authorization and authentication, monitoring and logging, interactive remote access, and security patch management.
7. **Physical Access Controls:** A review of CIP-006 and its strategic approach to preventing unauthorized access, as well as physical access controls, monitoring and logging approaches, and detail requirements of a visitor control program.
8. **Protecting BES Cyber System Information:** An audit of information protection program requirements for access control methodologies, access management and improper disclosure.
9. **Incident Response:** A synopsis on identifying an incident, appropriate notification procedures and CIP-008 reporting requirements.
10. **BES Cyber System Recovery:** A review of BES Cyber System recovery planning through the utilization of spare components, redundancy and restoration capabilities.
11. **CIP-014 Overview:** An examination of the physical security and assessment requirements required to identify and protect Transmission stations and Transmission Substations and their associated primary control centers as required by CIP-014.
12. **Conclusion:** A short wrap-up of CIP Cyber Security Training.

Cybersecurity risk is a people problem. Empower your people to be its solution.

www.sans.org/security-awareness-training/contact/

SANS SECURITY AWARENESS