SANS | GIAC CERTIFICATIONS

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

Empower a secure workforce with SANS

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 Workforce Security & Risk Training 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 Workforce NERC CIP Training is the most detailed, up-to-date curriculum addressing CIP V7 requirements on the market.

SANS Workforce 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 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.

SANS Workforce 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**
   This module welcomes you to the important roles and responsibilities of FERC, NERC, and the NERC Regional Entities. You'll also learn about the development of the NERC CIP Reliability Standards and the ways in which NERC Registered entities need to comply with these standards.

2. **Terms and Definitions**
   In this module, we'll give you a quick and easy walk-through of the key requirements.

3. **Operating Interconnected and Interdependent BES Cyber Systems**
   Explore the common components of these systems, how they work together, and their interdependence in achieving operational goals. We'll discuss cybersecurity risks to various components and explain the impacts of cybersecurity events, including the risks associated with Transient Cyber Assets and Removable Media.

4. **Asset Identification and Requirement Applicability**
   Standards Aligned: CIP-002
   Dive into the CIP-002 asset identification process and learn about the impact rating criteria approach included in Attachment 1. We'll cover the requirements, requirement parts, measures, and the detailed applicability approach taken with the CIP version 7 standards.

5. **NERC CIP Policy Requirements**
   Standards Aligned: CIP-003 CIP-004 CIP-007 CIP-010
   Take a tour of four key program policy areas required in CIP Version 7, including Personnel and Training, System Security Management, Configuration Change Management and Vulnerability Assessments, and Declaring and Responding to CIP Exceptional Circumstances.

6. **Electronic Access Controls**
   Standards Aligned: CIP-005
   This module will guide you through CIP-005, the Electronic Security Perimeter Standard. We'll cover authorization and authentication approaches, monitoring and logging, interactive remote access, and security patch management.

7. **Physical Access Controls**
   Standards Aligned: CIP-006
   Learn about CIP-006, the Physical Security of BES Cyber Systems Standard. We'll start with a strategy for protecting BES Cyber Systems from unauthorized access, then move on to physical access controls, monitoring and logging approaches, and the requirements of a visitor control program.

8. **Protecting BES Cyber System Information**
   Standards Aligned: CIP-011
   This module covers the essentials of an information protection program to ensure access control methodologies, managing access on a need-to-know basis, and handling improper disclosure.

9. **Incident Response**
   Standards Aligned: CIP-008
   We'll provide guidance on identifying an incident, the appropriate notification procedures, and the CIP-008 reporting requirements.

10. **BES Cyber System Recovery**
    Standards Aligned: CIP-009
    Explore the details of BES Cyber System recovery planning, including the use of spare components, redundancy, and restoration capabilities.

11. **CIP-014 Overview**
    Standards Aligned: CIP-014
    This module addresses the physical security and assessment requirements needed to identify and protect Transmission stations and Transmission Substations, along with their associated primary control centers as required by CIP-014.

12. **Conclusion:**
    A short wrap-up to the CIP Cyber Security Training.