ICS456: Essentials for NERC Critical Infrastructure Protection™

GCIP
Critical Infrastructure Protection
giac.org/gcip

5 Day Program | 31 CPEs | Laptop Required

You Will Be Able To

- Understand the cybersecurity objectives of the NERC CIP standards
- Understand the NERC regulatory framework, its source of authority, and the process for developing CIP standards, as well as their relationship to the other BES reliability standards
- Speak fluent NERC CIP and understand how seemingly similar terms can have significantly different meanings and impacts on your compliance program
- Break down the complexity to more easily identify and categorize BES Cyber Assets and Systems
- Develop better security management controls by understanding what makes for effective cybersecurity policies and procedures
- Understand physical and logical controls and monitoring requirements
- Make sense of the CIP-007 system management requirements and their relationship to CIP-010 configuration management requirements, and understand the multiple timelines for assessment and remediation of vulnerabilities
- Determine what makes for a sustainable personnel training and risk assessment program
- Develop strategies to protect and recover BES Cyber System information
- Know the keys to developing and maintaining evidence that demonstrates compliance and be prepared to be an active member of the audit support team
- Sharpen your CIP Ninja!

Hands-on Training

- **Section 1:** Set up your virtual environment, analyze network traffic, assess facility cybersecurity posture, and engage in a hands-on simulation to understand how operational and compliance decisions impact grid security.
- **Section 2:** Learn to analyze network traffic, configure firewalls, detect threats, and assess physical security risks—including lock picking—to strengthen both digital and physical defenses.
- **Section 3:** Assess system vulnerabilities, simulate real-world attacks, apply defensive measures, implement log management and change detection to secure critical assets.
- **Section 4:** Explore cyber threat intelligence techniques, uncover hidden data, detect malware, and test incident response readiness with a tabletop exercise you can take back to your team.
- **Section 5:** Use auditor-grade tools to analyze firewall configurations, leverage PowerShell for automation, and practice defending and articulating compliance strategies in a real-world audit scenario.

ICS456 training goes beyond the basics of NERC CIP by providing actionable strategies for compliance and security. You'll gain a deep understanding of the role of the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), and Regional Entities in enforcing reliability standards. The course provides multiple approaches for identifying and categorizing Bulk Electric System (BES) Cyber Systems, ensuring that asset owners can accurately scope and apply requirements to their unique environments. More than just a compliance course, ICS456 training bridges the gap between regulatory requirements and real-world security implementation. You'll explore practical strategies for securing industrial control systems (ICS) and operational technology (OT), balancing cybersecurity best practices with the realities of compliance.

Unlike other NERC CIP courses that focus only on the regulations, ICS456 immerses you in hands-on learning with 23 labs utilizing three dedicated virtual machines. These labs cover critical skills such as securing workstations, performing digital forensics, and even lock picking—because securing physical access is just as important as protecting digital assets. Our students consistently report that these interactive exercises reinforce learning and prepare them to apply their knowledge immediately on the job. By the end of this course, you won't just know what NERC CIP requires—you'll know how to implement its safeguards effectively, ensuring both compliance and a stronger security posture for the grid.

You Will Learn:

- BES Cyber System identification and strategies for lowering their impact rating
- Nuances of NERC-defined terms and the applicability of CIP standards and how subtle changes in definitions can have a big impact on your program
- The significance of properly determining cyber system impact ratings and strategies for minimizing compliance exposure
- Strategic implementation approaches for supporting technologies
- How to manage recurring tasks and strategies for CIP program maintenance
- Effective implementations for cyber and physical access controls
- How to break down the complexity of NERC CIP in order to communicate with your leadership
- What to expect in your next CIP audit, how to prepare supporting evidence, and how to avoid common pitfalls
- How to understand the most recent Standards Development Team's efforts and how that may impact your current CIP program

Authors' Statement

"The SANS ICS456: NERC Critical Infrastructure Protection Essentials course was developed by SANS ICS team members with extensive electric industry experience, including former Registered Entity Primary Contacts, a former NERC officer, and a Co-Chair of the NERC CIP Interpretation Drafting Team. Together the authors bring real-world, practitioner experience gained from developing and maintaining NERC CIP and NERC 693 compliance programs and actively participating in the standards development process."

—Tim Conway and Ted Gutierrez

Section Descriptions

SECTION 1: Asset Identification and Governance

A transition is under way from NERC CIP programs that are well defined and understood to a new CIP paradigm that expands its scope into additional environments and adds significantly more complexity. In Section 1, students will develop an understanding of the electricity sector regulatory structure and history as well as an appreciation for how the CIP standards fit into the overall framework of the reliability standards. Key NERC terms and definitions related to NERC CIP are reviewed using realistic concepts and examples that prepare students to better understand their meaning. We will explore multiple approaches to BES cyber asset identification and learn the critical role of strong management and governance controls. The section will examine a series of architectures, strategies, and difficult compliance questions in a way that highlights the reliability and cybersecurity strengths of particular approaches. Unique labs will include a scenario-based competition that helps bring the concepts to life and highlights the important role we play in defending the grid.

TOPICS: Regulatory History and Overview; NERC Functional Model; NERC Reliability Standards; CIP History; Terms and Definitions; CIP-002: BES Cyber System Categorization; CIP-003: Security Management Controls

SECTION 2: Access Control and Monitoring

Strong physical and cyber access controls are at the heart of any good cybersecurity program. During Section 2, we move beyond the "what" of CIP compliance to understanding the "why" and the "how." Firewalls, proxies, gateways, IDS and more—learn where and when they help and learn practical implementations to consider and designs to avoid. Physical protections include more than fences and you'll learn about the strengths and weaknesses of common physical controls and monitoring schemes. Labs will reinforce the learnings throughout the section and will introduce architecture review and analysis, firewall rules, IDS rules, compliance evidence demonstration, and physical security control reviews.

TOPICS: CIP-005: Electronic Security Perimeter(s); Interactive Remote Access; External Routable Communication and Electronic Access Points; CIP-006: Physical Security of BES Cyber Systems; Physical Security Plan; Visitor Control Programs; PACS Maintenance and Testing; CIP-014: Physical Security

SECTION 3: System Management

CIP-007 has consistently been one of the most violated standards going back to CIP version 1. With the CIP standards moving to a systematic approach with varying requirement applicability based on system impact rating, the industry now has new ways to design and architect system management approaches. Throughout Section 3, students will dive into CIP-007. We'll examine various Systems Security Management requirements with a focus on implementation examples and the associated compliance challenges. This section will also cover the CIP-010 requirements for configuration change management and vulnerability assessments that ensure systems are in a known state and under effective change control. We'll move through a series of labs that reinforce the topics covered from the perspective of the CIP practitioner responsible for implementation and testing.

TOPICS: CIP-007: System Management; Physical and Logical Ports; Patch Management; Malicious Code Prevention; Account Management; CIP-010: Configuration Change Management and Vulnerability Assessments; Change Management Program; Baseline Configuration Methodology; Change Management Alerting/Prevention

SECTION 4: Information Protection and Response

Education is key to every organization's success with NERC CIP and the students in ICS 456 will be knowledgeable advocates for CIP when they return to their place of work. Regardless of their role, all students can be a valued resource to their organization's CIP-004 training program, the CIP-011 information protection program. Students will be ready with resources for building and running strong awareness programs that reinforce the need for information protection and cybersecurity training. In Section 4 we'll examine CIP-008 and CIP-009 covering identification, classification, communication of incidents, and the various roles and responsibilities needed in an incident response or a disaster recovery event. Labs in Section 4 will introduce tools for ensuring file integrity and sanitization of files to be distributed, how to best utilize and communicate with the E-ISAC, and how to preserve incident data for future analysis.

TOPICS: CIP-004: Personnel and Training; Security Awareness Program; CIP Training Program; PRA Evaluation Process; CIP-011: Information Protection; Information Protection Program; Data Sanitization; CIP-008: Incident Reporting and Response Planning; Incident Response Plan/Testing; Reporting Requirements; CIP-009: Recovery Plans for BES Cyber Systems; Recovery Plans; System Backup

SECTION 5: The CIP Process

On the final section, students will learn the key components for running an effective CIP compliance program. We will review the NERC processes for standards development, violation penalty determination, Requests For Interpretation, and recent changes stemming from the Reliability Assurance Initiative. Additionally we'll identify recurring and audit-related processes that keep a CIP compliance program on track: culture of compliance, annual assessments, gap analysis, TFEs, and self-reporting. We'll also look at the challenge of preparing for NERC audits and provide tips to be prepared to demonstrate the awesome work your team is doing. Finally, we'll look at some real-life CIP violations and discuss what happened and the lessons we can take away. At the end of Section 5, students will have a strong call to action to participate in the ongoing development of CIP within their organization and in the industry overall as well as a sense that CIP is doable! Labs in Section 5 will cover DOE C2M2, audit tools, and an audit-focused take on a blue team/red team exercise.

TOPICS: CIP Processes for Maintaining Compliance; Preparing for an Audit; Audit Follow-Up; CIP Industry Activities; Standards Process; CIP of the Future

"This is a great course that examines NERC CIP standards and compliance from a variety of perspectives. I recommend it to anyone working with CIP."

—Tom Duffey, **Accenture Security**

Who Should Attend

- IT and OT (ICS) cybersecurity
- Field support personnel
- Security operations personnel
- Incident response personnel
- Compliance staff
- Team leaders
- Persons involved in governance
- Vendors/Integrators
- Auditors

NICE Framework Work Roles

- Privacy Officer/Privacy Compliance Manager (OPM 732)
- Process Control Engineer/ Instrument & Control Engineer (ZZ-ICS-001)
- ICS/SCADA Security Engineer (ZZ-ICS-002)
- ICS/OT Systems Engineer (ZZ-ICS-003)
- OT SOC Operator (ZZ-ICS-004)
- ICS/SCADA Security Engineer
- ICS/OT Systems Engineer
- OT SOC Operator

GCIP
Critical Infrastructure Protection
giac.org/gcip

GIAC Critical Infrastructure Protection

The GIAC Critical Infrastructure Protection (GCIP) certification validates that professionals who access, support and maintain critical systems have an understanding of the regulatory requirements of NERC CIP as well as practical implementation strategies.

- BES Cyber System identification and strategies for lowering their impact rating
- Nuances of NERC-defined terms and CIP standards applicability
- Strategic implementation approaches for supporting technologies
- Recurring tasks and strategies for CIP program maintenance