SANS CIP Version 5 Computer Based Training

What Is It?

SANS has developed a CIP Version 5 training program addressing the security of cyber assets essential to the reliable operation of the North American bulk electric system. The SANS CIP Version 5 CBT program specifically addresses the requirement parts of NERC CIP-004-5.1 R2 and the general security awareness requirements in CIP-004-5.1 R1.

- Explanation of differences between CIP Version 3 and 5
- Walk through of new and modified terms and definition introduced in CIP Version 5
- BES Cyber Assets Identification and Categorization
- All new or updated modules addressing:
    - √ Coverage of the nine security policy topics required by CIP-003-5 R1
    - √ Physical Access Controls
    - √ Electronic Access Controls
    - √ Visitor Control Program
    - √ BES Cyber System Information handling
    - √ Cyber Security Incident identification and response
    - √ BES Cyber System recovery
    - √ Risks of BES Cyber System interconnectivity & interoperability

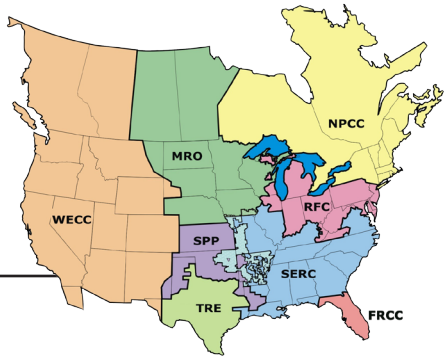
Program Benefits?

- Computer-based training enables employees to take training from any location.
- Short modular videos allow employees to complete training in multiple sessions as time permits.
- Training topics can be tailored to address specific audiences.
- Quiz questions after each module test learner comprehension.
- Progress reports enable tracking employee progress.

To learn more and to preview the Version 5 program, please email info@securingthehuman.org.

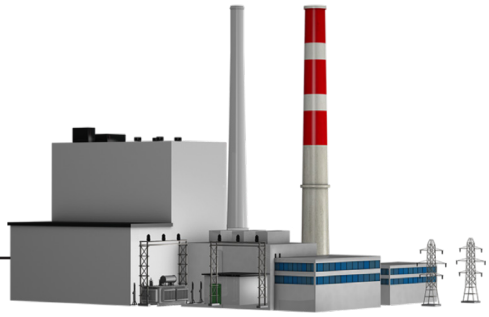
NERC CIP Foundations

- **Introduction** - introduces the roles and responsibilities of FERC and NERC, the standards development process and enforcement structure
- **Terms & Definitions** - reviews new and updated terms included throughout CIP Version 5
- **CIP Version 3 to Version 5 Delta** - An optional module explaining the significant changes in the Standard approach and methodology



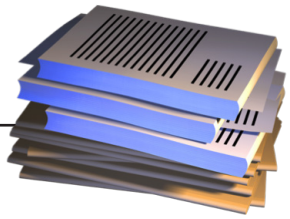
Reliability Impacts

- **Operating an Interconnected & Interdependent System** - details common Bulk Electric System components and how their operational design creates inherent risks
- **Asset Identification and Requirement Applicability** - details the complex process of identifying in-scope assets and categorizing based on potential impact to the Bulk Electric System



Governance

- **Policy Requirements** - walks through 4 key program policy areas including: Personnel and Training, System Security Management, Configuration Change Management and Vulnerability Assessments, and Declaring and Responding to CIP Exceptional Circumstances
- **Protecting BES Cyber System Information** - reviews the protection requirements, control methodologies, and handling of improper disclosure

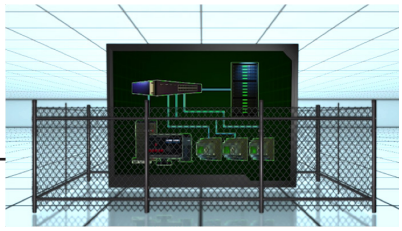


Access Controls

- **Electronic Access Controls** - reviews requirements and approaches to authorization/ authentication, event monitoring/logging, interactive remote access, and security patch management
- **Physical Access Controls** - presents approach and controls for protecting BES Cyber Systems from unauthorized physical access and reviews requirements for monitoring/ logging access as well as visitor controls

Incident Handling and Recovery

- **Incident Response** - provides guidance for the identification of an incident, appropriate notification procedures, and reporting requirements
- **BES Cyber System Recovery** - details system recovery planning through the use of spare components, redundancy, and restoration



Additional Training

- **CIP-014** - addresses the physical security and risk assessment requirements applicable to key Bulk Electric System substations and Control Centers