CENTER FOR CYBERSECURITY
AT THE UNIVERSITY OF WEST FLORIDA

NERC-CIP Standards—A Workforce Development Opportunity

CAE IN CYBERSECURITY COMMUNITY

Cybersecurity Education in Critical Infrastructure Protection (CECIP) Program

Project funded by a sub-award from the University of Memphis (sub-award A22-0041-S001) through an NCAE-C Program award (Award # H98230-21-1-0319)

The Need

- The U.S. Department of Energy in a report titled ***EERE*** [*] ***Cybersecurity Multiyear Program Plan*** underscores the need by stating

  > *" … the importance of addressing cybersecurity cohesively, improving cybersecurity defenses, and mitigating cyber vulnerabilities on energy supply infrastructures."*

- Find training solutions towards the protection of Critical Infrastructures with emphasis on Industrial Control Systems, Renewable Energy Systems, and Distributed Energy Resources
- Enable transitioning military, veterans, and active-duty military personnel to participate in Workforce Development programs in ICS, RES and DER security

[*] Energy Efficient and Renewable Energy

Workforce Development Training Opportunity

- Recognize the need to protect our critical infrastructures
- Compliance with the NERC-CIP Standards is a driving force in the electrical energy sector
- The NERC-CIP Standards could easily be adopted in other critical infrastructures
- Design and develop tabletop exercises and laboratory hands-on activities to support the training course
- Opportunity for upskilling and reskilling existing workforce towards filling the workforce gap of national significance

NERC-CIP

- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP)
- NERC-CIP Standards ensure the protection of assets used to operate North America’s Bulk Electric Systems (BES)
- Any entity that owns or operates any type of BES in North America must be in compliant with the standards
- As of October 2021, there are 12 enforceable standards, four subject to future enforcement, 1 pending to be inactive, and 78 are inactive.

NERC-CIP

- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP)
- NERC-CIP Standards ensure the protection of assets used to operate North America’s Bulk Electric Systems (BES)
- Any entity that owns or operates any type of BES in North America must be in compliant with the standards
- As of October 2021, there are 12 enforceable standards, four subject to future enforcement, 1 pending to be inactive, and 78 are inactive.

NERC-CIP Standards

CIP-002-5.1a Cyber Security - BES Cyber System Categorization
The Responsible Entity should have a process that identifies and categorizes all cyber assets according to their respective degree of impact to the reliable operation of the BES.

CIP-003-8 Cyber Security - Security Management Controls
Requires management controls that include the identification of CIP senior manager and authority delegation and the establishment of cyber security plans and policies

CIP-004-6 Cyber Security - Personnel and Training
This standard calls for the implementation of a periodic cybersecurity awareness training program and the establishment of personnel risk assessment and access management programs.

CIP-005-6 Cyber Security - Electronic Security Perimeter(s)
This standard requires that cyber assets on a network via routable protocol must reside within the Electronic Security Perimeter (ESP) and that external routable connectivity must go through an identified Electronic Access Point (EAP).

NERC-CIP Standards

CIP-006-6 Cyber Security - Physical Security of BES Cyber Systems
This standard requires a documented and implemented physical security plan that includes operational and procedural controls for restricted access.

CIP-007-6 Cyber Security - System Security Management
Requirements include securing manage ports and services, developing a sound patch management process, installing and maintaining methods to deter, detect, and prevent malicious code, implementing a security event monitoring system and a system access control.

CIP-008-6 Cyber Security - Incident Reporting and Response Planning
Requires an incident response plan to mitigate the risk to the reliable operation of a BES.

CIP-009-6 Cyber Security - Recovery Plans for BES Cyber Systems
Requires a recovery plan in support of the continued stability, operability, and reliability of a BES.

NERC-CIP Standards

CIP-010-3 Cyber Security - Configuration Change Management and Vulnerability Assessment
This standard requires the design and implementation of change management and vulnerability assessment processes.

CIP-011-2 Cyber Security - Information Protection
This standard requires that information, in transit or at rest, need to be protected through strong encryption techniques.

CIP-013-1 Cyber Security - Supply Chain Risk Management
This standard requires the implementation of processes that will identify and assess cybersecurity risks from vendor products or services, verify software integrity and authenticity of all software and patches provided by the vendor, and the coordination of access controls for vendors.

CIP-014-2 Physical Security
This standard requires the utility operators to perform initial and follow-up risk assessments on Transmission stations and substations.

Workforce Development Training Course

Learning Outcomes

Upon completion of the course, students should be able to:

- Describe in detail the 12 enforceable and 4 future enforceable NERC-CIP Standards
- Describe the compliance requirements of each of the 12 enforceable NERC-CIP Standards
- Map the NERC-CIP Standards to the NIST Cybersecurity Framework
- Apply cybersecurity tools (Nmap, Wireshark, Splunk, Snort, OpenVas, etc.) for verifying compliance
- Understand ICS physical and logical controls, security monitoring, security risk assessment, intrusion detection and prevention, and
- Analyze a given incident scenario transcript on a typical electric utility company

CENTER FOR **CYBERSECURITY**

AT THE UNIVERSITY OF WEST FLORIDA

Thank you!