Global Instrumentation and Control

# Network Architecture and Cyber Security: Cyber Security Training

## Background

Power plants around the world are faced with regulatory requirements established to ensure the safety of the plant, constituents, and the areas serviced. Cyber-attacks of networks and plant components present a real-world threat to safety and security.

Regardless of whether a site is beginning to implement a cyber security program, or whether it's been operating for years, an effective cyber security team is a well-trained and qualified one. Cyber security is a discipline of its own, and encompasses a range of topics, tools, and processes. A well-trained team will significantly increase the effectiveness of the site's cyber security program.

## Description

Westinghouse has designed cyber security training classes to address the unique needs and use cases required in Instrumentation and Control (I&C) systems. These training classes provide information needed to develop effective cyber security programs within both I&C facilities and the corporate network, and to become compliant with regulatory frameworks.

Westinghouse offers a variety of programmatic and technical training courses, ranging from establishing a cyber security program to network security and incident response to performing cyber security assessments. These courses are taught by certified cyber security professionals with operational, and where applicable, hands-on experience in the areas that they are providing instruction.

## Cyber Security Program Training

Westinghouse offers Cyber Security Program training, which assists licensees in establishing a cyber security program to operate at the site. This training is intended for Cyber Security Team members, including the management personnel who will be responsible for the cyber security program, and the program's executive sponsor.

Students will be educated in the following areas:

- **Cyber Security Plan** – The agreement between the governing organization and the licensee to establish the Cyber Security Program.
- **Cyber Security Team** – The management and engineering personnel who support and implement the cyber security program, maintain a positive security posture, evaluate changes to site equipment, and provide monitoring and incident response services.
- **Policies & Procedures** – The set of policies and procedures which implement cyber security throughout the system development lifecycle.
- **Cyber Security Awareness** – The program which focuses on providing awareness to site personnel about cyber security.
- **Cyber Security Program Maintenance** – The processes and programs that are involved with the ongoing operation of the cyber security program, including periodic effectiveness evaluations, risk evaluations, operational controls, qualifications, cyber event monitoring, and incident response.

Westinghouse

## Auditing and Assessment Training

The assessment process is a foundational component in understanding a site's security posture. These assessments assist in ensuring regulatory compliance, identifying areas of risk, and the development of a remediation plan to address the areas for improvement.

The Audit and Assessment Training course provides technical personnel and their direct managers the knowledge required to conduct cyber security audits and risk assessments.

Students will be educated in the following areas:

- **Cyber Security Assessment Team** – The team of auditors and assessors that will be answering the programmatic and technical cyber security controls, how to build the assessment team, and how to conduct effective assessment reviews.
- **Cyber Security Control Implementation Strategy (SCIS)** – The document that describes how the site should address the cyber security controls for all critical digital assets (CDAs), and provides an agreement upon the meaning and intent of the controls.
- **Assessment Concepts** – The concepts involved with conducting successful cyber security assessments, tabletop reviews and walkdown verifications, control types, control intent, control focus, threat vectors, and alternate controls. This module also discusses how to provide scoring to the controls, and how to write an effective observation.
- **Assessment Methodology** – The Westinghouse Assessment Methodology provides a significant time savings as compared to traditional one-by-one assessments. This module will provide students with an understanding of how to implement the methodology to increase the efficiency of assessments by leveraging commonalities between CDAs.
- **Lynx Risk Manager (LRM)** – The Westinghouse Assessment Methodology is implemented using a governance, risk and compliance (GRC) tool from Lynx Technology Partners. This module will provide students with an understanding of how the LRM tool works from both an assessor and administrator point of view using the assessment methodology.

## Cyber Security Specialist Training

The Cyber Security Team requires specialized cyber security training in order to be qualified to perform their responsibilities. This set of classes is designed to provide students with the skills and knowledge required to implement and maintain the cyber security program.

Each class consists of both presentation and hands-on components. Threat vectors, security concepts, controls and the associated risks are presented, and students gain operational experience with commonly used security products. Students are also provided the tools and instruction to learn how systems are manipulated when the security controls are not in place. The following classes are offered:

- **Operating System and Application Security –** Focuses on securing the endpoint and teaches the concepts of securing common desktop and server operating systems. Desktop administrators or cyber security team members will benefit from this class.
- **Network Security –** Focuses on controlling and monitoring network traffic by teaching the concepts of supporting firewall rules, access control lists and traffic signatures. Network administrators and cyber security team members will benefit from this class.
- **Monitoring and Incident Response –** Focuses on information gathering and analysis, and teaches the concepts of log correlation, digital forensics and incident response procedures. Incident response team members, staff responsible for log monitoring, or cyber security team members will benefit from this class.
- **Vulnerability Scanning and Virtualized Testing –** Focuses on finding vulnerabilities that may be exploited, and teaches the concepts of vulnerability detection and verification. Cyber security team members will benefit from this class.

## Benefits

Upon completion of these classes, students will understand the regulatory requirements for their site, and will be qualified to perform the roles associated with the Cyber Security Team members. All classes are taught by certified cyber security professionals with operational experience in the instructional areas.

Westinghouse Electric Company
1000 Westinghouse Drive
Cranberry Township, PA 16066

July 2019/ NA-0136