AMERICAN PUBLIC POWER ASSOCIATION

TRAINING SERVICES

JUNE 2020 CATALOG

Flexible Delivery. Expert Instructors. Cost Effective Approach.

AESI

Our Program

AESI offers a comprehensive list of training tailored to meet your Critical Infrastructure training needs. Our curriculum covers essential training for your utility's operational requirements and compliance obligations.

Our training is:

- Delivered onsite or online
- Designed to be interactive and engage the learner in active discussion on relevant industry trends
- Offered with training material that includes useful tools for your staff and business
- Enhanced industry case studies that reinforce key points

Our training is designed for all levels and departments:

- Board and Executive
- Senior Leadership
- Managers and Supervisors
- Operations Staff
- IT/Technical Staff

Select courses from a variety of categories:

- Governance and Risk Management
- Cybersecurity for Critical Infrastructure
- Cybersecurity Principles for IT/OT Environments
- Incident Response
- Privacy Programs
- Physical Security
- Distributed Energy Resources
- Regulatory Compliance

Courses at a Glance

GOVERNANCE AND RISK MANAGEMENT

Audience	Training Module Name	Duration
Board and Executive Senior Leadership	Cybersecurity: What Leaders Need to Know	1 hr
Board and Executive Senior Leadership Managers and Supervisors	Fundamentals of Information Security (with Workshop)	4 hrs
Board and Executive Senior Leadership Managers and Supervisors	Fundamentals of Information Security (without Workshop)	2 hrs
Managers and Supervisors	How to Develop and Implement Internal Controls	2 hrs
Senior Leadership	How to Determine and Define Cybersecurity Governance Roles In Your Organization	2 hrs
Senior Leadership	Effective Governance, Risk Management and Compliance Monitoring: How to Build a Cybersecurity Program That Actually Works	3 hrs

CYBERSECURITY FOR CRITICAL INFRASTRUCTURE

Audience	Training Module Name	Duration
All Levels and Departments	Putting Good Cyber Hygiene into Practice	2 hrs
All Levels and Departments	Supply Chain Risk Management Best Practices	2 hrs
Managers and Supervisors Operations Staff	Cybersecurity Best Practices	3 hrs

CYBERSECURITY PRINCIPLES FOR IT/OT ENVIRONMENTS

Audience	Training Module Name	Duration
IT/Technical Staff Managers and Supervisors	Fundamentals of IT/OT Cybersecurity Risk Management	3 hrs
IT/Technical Staff Managers and Supervisors	Best Practices for Planning and Maintaining Security Operations	3 hrs
IT/Technical Staff Managers and Supervisors	Access Management Concepts	3 hrs
IT/Technical Staff Managers and Supervisors	Securing Individual Hosts and Endpoints	3 hrs
IT/Technical Staff Managers and Supervisors	Risk Mitigation Strategies for Networks	3 hrs
IT/Technical Staff	Distributed Systems Security	1.5 hrs

INCIDENT RESPONSE

Audience	Training Module Name	Duration
All Levels and Departments	How to Develop Incident Response Policies and Procedures	3 hrs
IT/Technical Staff Operations Staff Managers and Supervisors	Technical Composition of an Incident Response Program	3 hrs
IT/Technical Staff Managers and Supervisors	Practical Table Top Exercises and Scenario Modeling	4-8 hrs

PRIVACY PROGRAMS

Audience	Training Module Name	Duration
Board and Executive Senior Leadership Managers and Supervisors	Understanding Privacy Programs	2 hrs

PHYSICAL SECURITY

Audience	Training Module Name	Duration
All Levels and Departments	Developing and Managing a Physical Security Plan	3 hrs

DISTRIBUTED ENERGY RESOURCES

Audience	Training Module Name	Duration
Distribution Planning Engineers and Managers	Distributed Energy Resources (DERs) Fundamentals	2 hrs

REGULATORY COMPLIANCE

Audience	Training Module Name	Duration
All Levels and Departments	Welcome to NERC Regulatory Compliance	1 hr
All Levels and Departments	Preparing for Your Audit	2 hrs
All Levels and Departments	Supply Chain Risk Management (NERC CIP-013)	2 hrs
All Levels and Departments	Cybersecurity Awareness Training for NERC Registered Entities	2 hrs
Board and Executive Senior Leadership Managers and Supervisors	Managing Your Compliance Obligations	1.5 hrs

Governance and Risk Management

Cybersecurity: What Leaders Need to Know

Duration: 1 hour
Who Should Attend: Board and Executive; Senior Leadership

As attempted attacks on utility infrastructure increase, it is important for everyone involved to understand the landscape and the terminology of cybersecurity.

Get an introduction to public power utility cybersecurity, learn about threats and breaches that have impacted utilities, and gain tips and tools to secure against these threats.

Fundamentals of Information Security

Duration with Workshop: 4 hours
Duration without Workshop: 2 hours
Who Should Attend: Board and Executive; Senior Leadership; Managers and Supervisors

According to the American Public Power Association (APPA), cybersecurity is among the top concerns that keep public power leaders up at night.

Designed to support the development and governance of a holistic cyber and physical security program, this in-person training session aims to help participants get started in creating the necessary building blocks specific to their utility. Training provides an understanding of key elements integral to the adoption and implementation of sound cybersecurity practices, including appropriate privacy controls, and any frameworks and/or standards that may be applicable.

Participants are engaged in the following topics:

- Crucial concepts of a holistic cybersecurity program
- Specific cyber risks, threat vectors, trends and recent incidents in the utility industry
- Overview of the necessary philosophy, culture of security and involvement of teams, including roles and responsibilities
- Governance perspectives for utility Board and Executive Teams
- Best practices for using a security blueprint for effective cyber risk management
- High level roadmap for a cybersecurity program and mitigation plan
- Guidance for developing a “next steps” plan with headcount and budgeting

This training is offered with or without an active participant workshop review of a utility case study.

How to Develop and Implement Internal Controls

Duration: 2 hours
Who Should Attend: Managers and Supervisors

This training session discusses how the establishment of Internal Controls help manage compliance activities and minimize the risk and impact of cybersecurity incidents.

Participants learn how to identify, create, articulate, and implement Internal Controls that will help drive compliance across your cybersecurity program.

How to Determine and Define Cybersecurity Governance Roles In Your Organization

Duration: 2 hours
Who Should Attend: Senior Leadership

Learn how to properly identify and assign accountability through the development of a RASCI Chart (Responsible, Accountable, Supporting, Consulted and Informed) and understand the importance of assigning accountability and responsibility for governance activities to ensure your security goals are met throughout your organization.

Effective Governance, Risk Management and Compliance Monitoring: How to Build a Cybersecurity Program that Actually Works

Duration: 3 hours
Who Should Attend: Senior Leadership

The objective of this module is to provide management direction and support for cybersecurity programs in accordance with business requirements, laws and regulations, and other identified criteria.

Participants learn how to apply effective program management practices such as the “Plan-Do-Check-Act" (PDCA) methodology as defined in the Deming Cycle.

Cybersecurity for Critical Infrastructure

Putting Good Cyber Hygiene into Practice

Duration: 2 hours
Who Should Attend: All Levels and Departments

Focus is on administrative and operational staff, management, and contractors, to inform and raise awareness of general security concepts and industry best practices regarding safeguarding IT assets.

Participants will practice techniques to better protect themselves and their organization from social engineering and other threats.

- How to implement good password management
- How to employ safe and secure email practices
- How to recognize and react to ransomware

Supply Chain Risk Management Best Practices

Duration: 2 hours
Who Should Attend: All Levels and Departments

Third party providers can introduce unforeseen risk into your IT/OT environment through unmitigated vulnerabilities and ineffective or nonexistent cyber policies.

In this course, participants will learn how to identify and manage Supply Chain risks and how to implement security controls and metrics that will help reduce and manage risks and vulnerabilities that originate from vendors.

Cyber Security Best Practices

Duration: 3 hours
Who Should Attend: Managers and Supervisors; Operations Staff

Focus is on managers, supervisors and staff responsible for supporting the operations of Critical Infrastructure assets, and who may be required to logically or physically access these assets or information about them.

This session will:

- Reinforce the importance of cybersecurity practices
- Reinforce the obligations of managers and supervisors in the protection of Critical Infrastructure assets
- Demonstrate the basic techniques to mitigate threats
- Illustrate non-compliant activities that should be eliminated

Cybersecurity Principles for IT/OT Environments

Fundamentals of IT/OT Cybersecurity Risk Management

Duration: 3 hours
Who Should Attend: IT/Technical Staff; Managers and Supervisors

Focus is on IT/OT staff responsible for operating and maintaining Critical Infrastructure assets.

This course will outline basic risk management techniques and discuss governance, policy, organizational and technical considerations.

Participants will learn how to:

- Define sound security policy and governance models based on risk assessment
- Integrate risk-based policies with legal and regulatory requirements
- Describe cyber and physical security concepts for utilities
- Build a Cybersecurity Roadmap
- Implement technical controls for critical cyber assets
- Appropriately manage risk and reduce exposure

Best Practices for Planning and Maintaining Security Operations

Duration: 3 hours
Who Should Attend: IT/Technical Staff; Managers and Supervisors

Attendees will be able to successfully:

- Develop a Cybersecurity Management and Operations Plan
- Understand the differences between a Disaster Recovery Plan and a Business Continuity Plan
- Understand basic security practices that should be used in an IT/OT environment
- Develop a high level continuity of operations strategy

Access Management Concepts

Duration: 3 hours
Who Should Attend: IT/Technical Staff; Managers and Supervisors

In this training, participants develop and understand their utility attack surface and identify user-related risks and related mitigation strategies.

Authentication and access management concepts are discussed and appropriate countermeasures are outlined for utility use in minimizing impacts of user errors and malicious acts.

Participants will discuss the benefits and pitfalls of single sign-on systems and learn best practices for user-management processes.

Securing Individual Hosts and Endpoints

Duration: 3 hours
Who Should Attend: IT/Technical Staff; Managers and Supervisors

With many employees working remotely, the enterprise network now extends into lightly defended and mostly untrusted personal area networks.

This model has increased the organization's attack surface and consequently the opportunity for a cyber breach.

Participants learn techniques that can be used to secure hosts and endpoints, and apply multi-layered approaches to securing virtual workspaces. Virtual Desktop Infrastructure (VDI) tools are reviewed and participants develop better understanding of how to protect themselves when working outside of their controlled enterprise network.

Risk Mitigation Strategies for Networks

Duration: 3 hours
Who Should Attend: IT/Technical Staff; Managers and Supervisors

Participants will discuss network architecture concepts and identify key tools that can be used to mitigate risk. Participants will also learn why using monitoring and surveillance tools are not enough.

Using a Defense-in-Depth reference architecture, participants design a network security architecture that reduces risk while maintaining reliability and performance.

Distributed Systems Security

Duration: 1.5 hours
Who Should Attend: IT/Technical Staff

This module is an advanced-level survey of modern topics in computer security focusing on distributed systems, applied cryptography, distributed access control, mobile code, key management, and networks. Common attack techniques such as ransomware, phishing, masquerading and identity hijacking are discussed.

Incident Response

How To Develop Incident Response Policies and Procedures

Duration: 3 hours
Who Should Attend: All Levels and Departments

Comprehensive Incident Response (IR) plans lay down the steps that an organization should take to recognize, respond to, and recover from various types of cyber incidents and their potential impacts.

IR plans include six (6) key activities:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Follow Up

This module will discuss these key activities and recommended documentation that should be in place to mitigate impacts to the business and quickly recover services.

Policy and procedure examples include:

- Incident Recognition and Categorization
- Internal and External Communications
- Legal and Law Enforcement Involvement
- Asset Inventories and Classification
- Data Governance, Backup and Restoration
- Site Safety and Emergency Response
- Reporting and Escalation
- Quarantine Procedures
- Safe Startup and Shutdown
- Baseline Restoration
- File and System Integrity Management
- Evidence Collection, Protection and Chain of Custody
- Closeout

Technical Composition of an Incident Response Program

Duration: 3 hours
Who Should Attend: IT/Technical Staff; Operations Staff; Managers and Supervisors

This module discusses the technical components of an incident response program that enhance the survivability of an organization, including:

- Detective Controls: Monitoring and Surveillance
- Alerting and Notifications
- Protective Controls: Automated and Manual Countermeasures and Interventions
- Corrective Controls: Fault Tolerance, Redundancy, Failover and Service Restoration
- Incident Closeout and Lessons Learned

Participants will also engage in exercises where they will:

- Construct an Incident Response model
- Apply the Incident Response model to simulated cyber and physical security incidents
- Practice program implementation, management and close out

Practical Table Top Exercises and Scenario Modeling

Duration: 4-8 hours
Who Should Attend: IT/Technical Staff; Managers and Supervisors

AESI's Cybersecurity Exercise (CX) Program is an intellectually intensive exercise that explores the effects of cyber offensive operations on the capability of targets or victims to continue operations during and after a cyber incident. We develop wargame-like exercises that focus on two teams with opposing missions:

- An adversarial "Red Team" charged with carrying out a compromise against one or more assets
- A defensive "Blue Team" charged with protecting and defending those assets

Our CX framework combines methods described in NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, and methods from the Sandia National Laboratory (SNL) Information Design Assurance Red Team (IDART™) methodology, which was initially developed to assess and protect the United States' nuclear arsenal and is now adapted for cyber security. Members of our team are certified in the IDART method.

The CX provides System Engineers, Program Managers, Information System Security Managers, Information System Security Engineers, Testers, and other Analysts with actionable information on cyber threats, including potential system vulnerabilities, demonstrated means of exploitation of those vulnerabilities, and an assessment of the resulting impacts. This information enables leaders to allocate limited resources more effectively to deliver a system that will operate successfully in a cyber-contested environment.

Privacy Programs

Understanding Privacy Programs

Duration: 2 hours
Who Should Attend: Board and Executive; Senior Leadership; Managers and Supervisors

This course outlines how to implement a Privacy Program that includes the important protection controls to meet your desired goals of information control, breach prevention and creation of processes for responding to data privacy-related events. The objective is to provide participants with information that will aid in improving your Privacy Program and posture with the incorporation of activities that enable organizational control of the full lifecycle of information.

Key topics of discussion in this course include:

- Understanding the Privacy threat landscape, including how cybersecurity and privacy are intertwined
- Aligning with applicable jurisdictional privacy regulations and guidelines
- When to employ Privacy concepts such as NIST SP 800-37, a risk management standard incorporating privacy, or a framework such as Privacy by Design (which is applicable for utility grid environments)
- Specific focus on Personal Identifiable Information (PII) and protection of employee/customer personal data for utilities
- Key factors for executing a successful privacy program

Physical Security

Developing and Managing a Physical Security Plan

Duration: 3 hours
Who Should Attend: All Levels and Departments

Our approach to assessing and managing physical security leverages a layered countermeasure and intrusion containment model that evaluates physically separated operating zones, each with specific layered controls that become more restrictive as zones are penetrated. Learn how to evaluate and design physical security controls from the perspective of facility and personnel protection using proven Red Team offensive testing approaches.

In this course participants:

- Learn about designing modern, effective security countermeasures that protect Critical Infrastructure facilities and ensure staff and visitor safety
- Discuss methods to physically secure environments to maintain the safety of the public and to mitigate issues that could result in legal action
- Discuss methods to maintain the integrity of business and technical operations, such as ensuring the supply of electricity and safe drinking water for customers
- Discuss ways to minimize reputational risk to your organization
- Explore methods used to minimize potential financial impacts that could result due to theft of equipment, damage to property, and outages to the delivery of essential services

Distributed Energy Resources

Distributed Energy Resources (DERs) Fundamentals

Duration: 2 hours
Who Should Attend: Distribution Planning Engineers and Managers

The evolution of the energy market is accelerating in the direction of a greater reliance upon distributed energy resources (DER), whether those resources generate, consume, or store electricity. The technologies and new frameworks necessary to manage this increasing two-way complexity can be challenging to navigate. Nevertheless, successful strategies to harvest more value from smaller, cleaner, and smarter energy resources are being deployed today.

In this course, we explore the following topics:

- What are Distributed Energy Resources (DERs)
- How do we introduce, integrate, and operate DERs
- What benefits and challenges do DERs bring to the energy market

Participants will engage in a review of case studies and explore the advantages and disadvantages of DERs, discussing also the current trends in the energy market as they relate to DERs.

Regulatory Compliance

Welcome to NERC Reliability Compliance

Duration: 1 hour
Who Should Attend: All Levels and Departments

This course introduces participants to the world of NERC Reliability Compliance.

Participants learn how NERC was formed and its evolution into becoming the Electric Reliability Organization (ERO) for North America.

Participants will also:

- Explore the roles of FERC, Regional Entities and Functional Entities
- Learn what it means to be considered part of the Bulk Electric System (BES)
- Discover the many families of reliability standards
- Understand how the reliability standards are developed and adopted, and how the industry can mold and shape requirements
- Learn the various compliance enforcement mechanisms that exist and of the potential consequences of non-compliance

Preparing for Your Audit

Duration: 2 hours
Who Should Attend: All Levels and Departments

Being well prepared for an audit is key to a smooth and successful audit engagement. This course teaches participants how to prepare their operations, documentation and evidence, and staff to effectively navigate the audit process.

This course will:

- Describe the audit process
- Explain the Reliability Standard Audit Worksheets (RSAWs)
- Teach participants how to best draft and structure RSAW narratives
- Help prepare “witnesses” or Subject Matter Experts (SMEs) for their audit interviews

Supply Chain Risk Management (NERC CIP-013)

Duration: 2 hours
Who Should Attend: All Levels and Departments

NERC CIP-013 requires Registered Entities to address cybersecurity Supply Chain Risk Management for industrial control system hardware, software, computing and networking services associated with Bulk Electric System (BES) operations.

Participants learn how to mitigate cybersecurity risks to the reliable operation of the BES by implementing a supply chain risk management plan. This course presents processes that ensure cybersecurity risks are identified and managed throughout the lifecycle of the product and/or service and demonstrates how to integrate required controls into existing processes.

Cybersecurity Awareness Training for NERC Registered Entities

Duration: 2 hours
Who Should Attend: All Levels and Departments

Focus is on entities subject to NERC regulatory requirements to inform and raise awareness of current security concepts and industry best practices regarding safeguarding IT/OT assets.

Participants will learn:

- Techniques to better protect themselves and their organization from social engineering and other threats
- Current CIP requirements for cybersecurity and physical security
- How to manage transient cyber assets and removable media
- How to reduce risks introduced by privilege escalation
- The Do’s and Don’ts of Remote Access

Managing Your Compliance Obligations

Duration: 1.5 hours
Who Should Attend: Board and Executive; Senior Leadership; Managers and Supervisors

Learn how to cultivate a good culture of compliance and reliability, reduce the instances of compliance fatigue, and minimize the risks to compliance by better managing your NERC compliance obligations.

Participants are taught the fundamental tenets of an Internal Compliance Program based on industry best practice. Topics of discussion include, but are not limited to:

- Understanding why there are compliance violations
- Organizational structure to support a culture of compliance
- Compliance documentation framework
- Compliance awareness and training
- Tools and systems for proactive compliance
- Internal controls to minimize the risks to compliance
- Monitoring and self-assessment of current compliance posture
- Regulatory and industry awareness and participation

INDUSTRY'S TRUSTED ADVISOR.

Proven. Credible. Reputable.

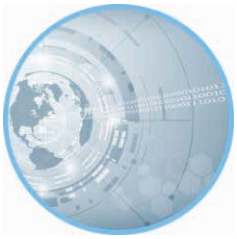
AESI is an engineering and management consulting firm providing pragmatic and sustainable engineering, technical and management solutions to utilities, government agencies, commercial and industrial entities, and institutions (i.e., Critical Infrastructure) across North America, and internationally, helping them maintain reliable operations, meet regulatory requirements, and harness technology to attain operational excellence.

REGULATORY COMPLIANCE

Compliance Assurance Services
Compliance Advisory Services
Compliance Implementation Services
Managed Compliance Services

OPERATIONAL TECHNOLOGY

IT/OT Assessments & Analysis
Complete OT Lifecycle Advisory & Management Services
System Implementation & Configuration
Sustainment & Maintenance



CYBER SECURITY

Cyber Security Risk Assessments
Cyber Security Advisory Services
Cyber Security Implementation Services
Cyber Security Managed Services

ENERGY SOLUTIONS

Energy Advisory Services
Engineering Services
Distributed Energy Resource Implementation
Operations & Planning Services

LEARN MORE:

aesi@aesi-inc.com www.aesi-inc.com

AESI