

2026

CYBERSECURITY TRAINING COURSES

FEMA

Contents

3
About the NCPC

4
NCPC Experience
A snapshot of the NCPC partners and where they've trained participants.

6
AWARENESS Courses
These courses provide a general awareness of various topics within cybersecurity.

13
COORDINATION & PLANNING Courses
These courses are ideal for organizations and communities preparing for physical and cyber threats.

17
CYBER INCIDENT RESPONSE and RECOVERY Courses
Incident response teams, IT Personnel and any organization coordinating and/or managing cyber-related incident response and recovery will want to participate in these courses.

20
TECHNICAL Courses
Ranging from basic- to advanced-level, these courses help technical personnel protect network infrastructures from various cyber threats.

25
CYBER THREAT INFORMATION SHARING Courses
These courses are designed to help you establish an information sharing capability and become more familiar with the cyber threat information sharing ecosystem.

To see all NCPC courses, visit our website >>

About the NCPC

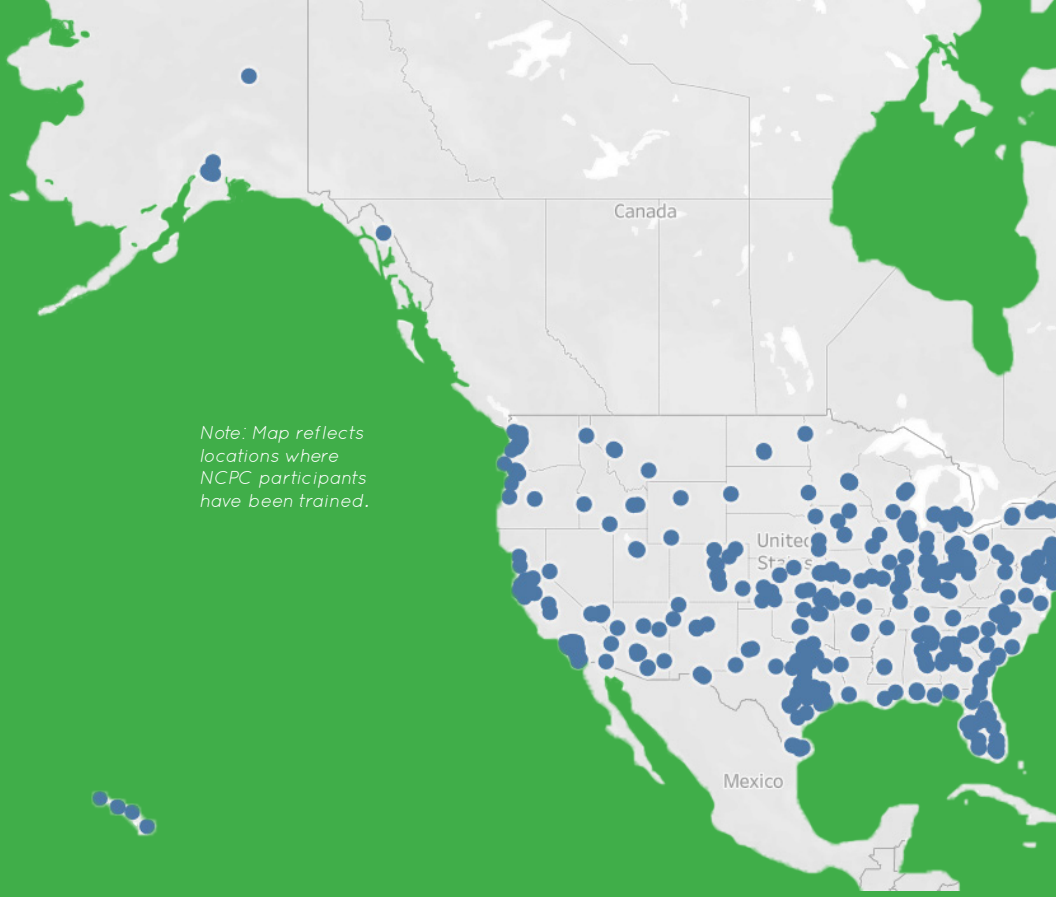
The mission of the National Cybersecurity Preparedness Consortium (NCPC) is to provide research-based, cybersecurity-related training, exercises, and technical assistance to local jurisdictions, counties, states, tribes, territories and the private sector.

Using the Community Cyber Security Maturity Model (CCSMM) as a basis from which to work, the consortium collectively works with states and communities as they progress through the model.

The CCSMM is based on over a decade of experience with states and communities working to develop viable and sustainable cybersecurity programs for the whole community.

To register for NCPC web-based and instructor-led courses, contact your state's Homeland Security Training Office. More information on how to register for courses is on **NationalCPC.org**.

FEMA



Note: Map reflects locations where NCPC participants have been trained.

By the Numbers

As of September 30, 2026, members of the Consortium have trained more than 174,043 participants:

- CJI – 10,525 trained
- CIAS – 11,264 trained
- TEEX/NERRTC – 140,315 trained
- CfIA – 8,243 trained
- NUARI – 3,696 trained

NCPC Experience

As early as 2004, in partnership with the Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA), the individual members of the NCPC have developed and delivered DHS/FEMA certified online and face-to-face **no cost** training courses to an array of states, counties, local jurisdictions, and critical infrastructure components nationwide addressing cybersecurity concerns.

NCPC Partners

Criminal Justice Institute (CJI), University of Arkansas System | cdi@cji.edu

Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio | cias@utsa.edu

Texas A&M Engineering Extension Service/National Emergency Response and Recovery Training Center (TEEX/NERRTC) | bcs@teex.tamu.edu

University of Memphis, Center for Information Assurance (CfIA) | cfia@memphis.edu

Norwich University Applied Research Institutes (NUARI) | nuaritraining@nuari.org



Awareness

Cyber Ethics (AWR-174-W)

WEB-BASED. 13 hours; 1.3 CEUs; 1 hour - ACE; 2 semester hours.

This course shares the proper techniques for approaching the difficult ethical dilemmas arising from use of the modern Internet. Develop the skills to assess future ethical dilemmas by examining some of the more pressing concerns related to Internet usage today.

Cyber Security Awareness for Municipal, Police, Fire & EMS IT Personnel (AWR-388-W)

WEB-BASED. 2 hours.

This course provides participants with an increased knowledge of threats specific to their jurisdiction and an understanding of the processes and procedures needed to develop a cyber-awareness program. It focuses on the steps involved in being aware of cyber threats and effectively communicating the processes and procedures to protect users against common cyber threats.

LEGEND / KEY

- Web-Based Course
- Instructor-Led Course
- COMING SOON — Courses Under Development
- Information Technology
- End User
- Management/ Leadership

Cybercrime Insight and Introduction to Digital Evidence Identification (AWR-427)

INSTRUCTOR-LED. 8 hours.

A course that introduces state, local, tribal and territorial first responders with limited or no prior knowledge of computer crime and cyber investigations to the importance of identifying evidence related to suspected criminal activity, and incorporating evidence into investigation.

Cybersecurity Risk Awareness for Officials and Senior Management (AWR-383)

INSTRUCTOR-LED. 4 hours; .4 CEUs.

This course is designed to develop awareness of cybersecurity risks for elected officials, appointed officials and other senior managers so that they are better informed to properly protect the jurisdiction/organization during a cybersecurity incident.

Cybersecurity for Everyone (AWR-397-W)

WEB-BASED. 4 hours; .4 CEUs.

This course introduces participants to the basics of protecting their computer and the data it stores, as well as how to protect themselves when online, on social media and while using a mobile or smart device.

Cybersecurity in the Workplace (AWR-395-W)

WEB-BASED. 2 hours; .2 CEUs.

This course helps participants understand the different types of cyber-attacks their company may face, the type of information that is at risk, how to recognize cyber-attacks and why it is important for everyone in the organization to participate in cybersecurity.

Critical Thinking and Risk Management in a Cyber-Converged World (MGT-328)

INSTRUCTOR-LED. 4 hours.

This ccourse enables leaders to define and determine business risk related to cybersecurity in a multi-dimensional environment. Students are exposed to complex analysis and decision making with consideration of converged catalysts (e.g., cyber, physical, informational) impacting operations. They will gain an appreciation for a standard taxonomy and introduced to methods to calculate risk. The course is based on Factor Analysis of Information Risk (FAIR) but does not purport to cover FAIR in its entirety.

Awareness



Cybersecurity for Educational Leaders (AWR-301)



INSTRUCTOR-LED. 8 hours.

Educational institutions of all sizes (including higher education and K-12) are data rich, making them targets for cyber-attacks. Cybersecurity readiness is not solely a technology issue; it includes managing student safety, well-being and digital risks. This non-technical course will introduce key cybersecurity concerns for leaders and will foster discussions to build strategies of cybersecurity preparedness to ensure adequate resources are considered to meet data privacy and cybersecurity needs.



Detecting and Responding to a Cyber Attack (AWR-399-W)



WEB-BASED. 4 hours; .4 CEUs.

This course introduces students to varous types of cyber-attacks and how to detect and respond to them in order to protect their data and information.



Demystifying Cybersecurity Attacks: A Grey Hat Lab (PER-400)



INSTRUCTOR-LED. 8 hours.

This course demonstrates tools used by bad actors and cyber defenders to provide a complete picture of a cyber-attack. This course is ideal for any individual responsible for responding to cyber incidents or organizational strategy.



Foundations of Cyber Crimes (AWR-168-W)

WEB-BASED. 10 hours; 1.0 CEUs; 2 semester hours



This course examines cyber and cyber facilitated non-violent white-collar crimes, fraud and financial crimes, and violent crimes, and the appropriate response by first responders and other local, state and federal agencies that may encounter them. Participants will identify legislative, organizational and suggested personal efforts to control or prevent cyber crimes.

Internet of Things Security (PER-301)

INSTRUCTOR-LED. 32 hours

Designed to provide knowledge and skills to a targeted audience of information technology practitioners about the importance of IoT in society, the current components of typical IoT implementations and trends for the future. The course will cover IoT design considerations, constraints and interfacing between the physical world and a very large variety of devices that have not traditionally been considered as part of the IT Security problem. It will also cover key components of networking to ensure that students understand how IoT devices can be properly and securely connected to the Internet.

Introduction to Internet of Things (AWR-402-W)

WEB-BASED. 3 hours; .2 CEUs.

This course provides an understanding of the history, definitions and components that make up IoT. It addresses the different applications of IoT, as well as applicable laws and policies, technologies, emerging threats, best practices, security and a variety of existing and developing technologies. This course is ideal for participants, from throughout the various levels of government, private industry and community, wanting to understand how they are affected by IoT.

Mobile Device Security & Privacy (AWR-385-W)

WEB-BASED. 6.5 hours.

This course is designed to provide a better understanding of security and privacy issues associated with mobile devices and infrastructure; including benefits and challenges of designing, implementing and maintaining Bring Your Own Device (BYOD) Programs. Using scenarios, thought challenges and exercises as a framework, students will learn about the purpose of Enterprise Mobile Management platforms; elements that make mobile networks and operating systems different Mobile malware classifications and detection strategies; and mobile architecture data leakage detection and prevention strategies.

KEY

Web-Based Course

Instructor-Led Course

COMING SOON
Courses Under Development

Information Technology

End User

Management/ Leadership

Network Security for Homes and Small Businesses (AWR-396-W)

WEB-BASED. 2 hours; .2 CEUs.

This course introduces students to the basics of networks for homes and small businesses, and provides them with best practices to secure their networks in order to protect their personal information as well as other information (e.g., friends, family, customerrs, vendors) that may flow through their network.

Practical Internet of Things (IoT) Security (AWR-428)

INSTRUCTOR-LED. 8 hours.

This course introduces students to components of an IoT system and associated security concerns. It covers the elements of an IoT system, including programmable logic controllers, sensors and network interfaces. Students explore IoT vulnerabilities using common vulnerability assessment tools, along with lectures and exercises culminating in a laboratory experience.

Remote/Home-Office Cybersecurity Preparedness (RHC) (AWR-431-W)

WEB-BASED. 4-6 hours.

This course addresses the changing workforce, opening the door for remote work environments that are changing the landscape of cybersecurity and Work From Home (WFH) strategies. The need for home office and normal work strategy/infrastructures is becoming tightly coupled, requiring using different cyber-enabled systems, devices and services.

Understanding Social Engineering Attacks (AWR-367-W)

WEB-BASED. 8 hours.

This course educates the public in the general understanding and some common defense tactics that can be used to mitigate social engineering attacks. It provides an understanding of how social engineering attacks can be better mitigated by combining comprehensive security measures with an understanding and awareness of how such attacks can exploit human behaviors. This course introduces phishing, spear-phishing, water-holing, ransomware and other types of advanced persistent threats.

Understanding Targeted Cyber Attacks (AWR-376)

INSTRUCTOR-LED. 8 hours; .8 CEUs.

This course provides specific information regarding targeted cyber attacks, including advanced persistent threats. This information will place participants in a better position to plan and prepare for, respond to and recover from targeted cyber attacks. This course fills the gap in threat-specific training for cybersecurity as a community-driven course that focuses on the phases of targeted cyber attacks and the attacker methods used during each phase. Participants will also receive valuable information on cyber attack prevention, mitigation and response.

Cybersecurity in Cloud Environments (AWR-361-W)

WEB-BASED. 4 hours.

COMING SOON

The proliferation of cloud computing continues to grow as organizations look to reduce the cost of operating and maintaining traditional information technology (IT) data centers and associated IT resources. To overcome the limitation and drawbacks of existing approaches and to fill in technical gaps, this web-based course includes topics such as understanding different cloud security architectures; emerging threats to cloud security; and how to properly configure and manage cloud-based assets to protect them against compromise.

Cybersecurity in Operational Technology (AWR-374-W)

WEB-BASED. 6 hours

COMING SOON

This awareness level course is designed to address the technical needs of future workforce and industry professionals in various sectors, including electric vehicle charging stations (EVCS). General topics to be covered include: understanding various cyberattacks and their negative impacts on OTs and charging systems; OT threat actors; OT security measures for both Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA); detecting cyberattacks on the OTs; and security best practices.

Cybersecurity Issues in Distributed Energy Resources (DER's) (AWR-373-W)

WEB-BASED. 6 hours

Awareness level course designed to assess the current state of cybersecurity standards and develop methods for the grid-connected DERs under cyber threats for enhanced resiliency by applying appropriate physics-driven real-time monitoring and advanced data analytics, including machine learning and artificial intelligence on observed data.

Security in Operational Technology and Distributed Energy Resources: Tools and Applications (MGT-363)

INSTRUCTOR-LED. 8 hours.

This performance level course designed to provide hands-on content/labs. The hands-on activities will cover some topics from the security in operational technology (OT) course and some topics from cybersecurity in distributed energy resource (DER) course. This is important for state and local professionals and employees in specific sectors to transition theory to practice to more effectively deal with cybersecurity challenges.

Cybersecurity in Supply Chain Operations (MGT-354)

INSTRUCTOR-LED. 16 hours.

Supply chains are increasingly targeted by sophisticated cyber-attacks due to their complexity and the valuable of the data they handle, making cybersecurity a critical concern for ensuring the continuity and resilience of supply chain operations. Integrating cybersecurity training into supply chain management is critical to safeguarding against the increasing threat of cyberattacks.

Coordination & Planning

Community Cybersecurity Preparedness Simulation (MGT-301)

INSTRUCTOR-LED. 8 hours.

This course is designed as a tabletop activity simulating a community-wide cybersecurity event. Using a gamification approach, participants will strategize with a diverse group of stakeholders to plan for and respond from a cybersecurity incident that could have cascading effects across the community. Specifically, this training will encourage participants to discuss budgeting and planning strategies; coordinate with other community stakeholders to respond to a cyber incident; and will inform participants of various recovery aspects that may be included in a cybersecurity program.

Community-Level Cybersecurity Planning and Training Gap Analysis (MGT-362)

INSTRUCTOR-LED. 16 hours.

Designed as a collaborative community approach to identifying the gaps in cyber plans and the training needed in cybersecurity for all levels of community personnel and local critical infrastructure partners. At the end of this course, participants will be able to conduct a community cybersecurity gap analysis resulting in a cybersecurity training plan for all levels of community personnel and local critical infrastructure partners.



Coordination & Planning



Cybersecurity in a Resource Constrained Environment for Public and Rural Electricity Providers (PER-338)

INSTRUCTOR-LED. 16 hours

Cybersecurity preparedness and response in a resource-constrained enterprise, partnering Information Technology with Operational Technology security and operations professionals, and with a detailed focus on the business and regulatory environment that public and rural electricity providers experience.



Cybersecurity Vulnerability Assessment (MGT-303)

INSTRUCTOR-LED. 16 hours.

Through learning to conduct cybersecurity vulnerability assessments and developing a vulnerability remediation program, organizations will be able to prepare and plan for cyber incidents. Activities include examining, analyzing, and prioritizing assets, risks and vulnerabilities to develop a vulnerability assessment report that could be delivered to organizational leadership.



Identifying, Prioritizing, and Assessing High Value Assets (PER-342)

INSTRUCTOR-LED. 8 hours.

Every organization has critical information and technology assets that are essential to their business operations and require enhanced security. Organizational resources that can be dedicated to cybersecurity are finite; therefore, those resources should be applied deliberately and strategically focusing on the most important assets. This course will enable participants to identify their high value assets, prioritize them, assess them and create a remediation action plan. This is designed to align with the Federal HVA Program but provides a scalable and flexible approach that will assist any size SLTT organization to identify their critical assets based on their individual requirements.

Integrating Cyber Hazard Response into Exercise Planning (AWR-432)

INSTRUCTOR-LED. 4 hours

This course is designed to introduce state, local, tribal and territorial exercise planners with limited or no prior knowledge of integrating cyber hazards and their relationship to planning exercises related to cyber-enabled threats. This is an awareness-level course that will help exercise planners to properly develop exercises using major cyber threats to reduce cybersecurity risks and impacts to critical infrastructure.

Organizational Cybersecurity Policy Essentials (MGT-333-W)

WEB-BASED. 4 hours.

This course is designed to provide students with a process for development of cybersecurity policies. Students will learn six key tasks to consider when developing policies, basic structure of a cybersecurity policy, and the types of cybersecurity policies an organization should consider. In this course, students will understand how to develop and implement cybersecurity policies that address cybersecurity practices and controls needed for their organization.

Physical and Cybersecurity for Critical Infrastructure (MGT-452)

INSTRUCTOR-LED. 8 hours; .8 CEUs.

This course encourages collaboration efforts among individuals and organizations responsible for both physical and cybersecurity toward development of integrated risk management strategies that lead to enhanced capabilities necessary for the protection of our nation's critical infrastructure. Participants will identify physical and cybersecurity concerns impacting overall infrastructure security posture, examine integrated physical and cybersecurity incidents and the evolving risks and impacts they pose to critical infrastructure.

Preparing for Cyber Attacks and Incidents (MGT-384)

INSTRUCTOR-LED. 16 hours; 1.6 CEUs.

This non-technical course is designed to prepare organizations and communities for the next cyber attack or incident. Participants will analyze cyber threats, vulnerabilities, and initial and cascading impacts of cyber attacks and incidents, evaluate the process for developing a cyber preparedness program, examine the importance and challenges of cyber related information sharing and discover low to no cost resources to help build cyber resilience.

Coordination & Planning



Using the Community Cyber Security Maturity Model to Develop a Cyber Security Program (MGT-364-W)

WEB-BASED. 3.5 hours.

This course will enable community leaders, network/security personnel and those individuals involved in developing or maintaining plans used for and throughout the community. Participants will understand what is required to develop a coordinated, sustained and viable community cybersecurity program. Participants will be introduced to various resources, including the Community Cyber Security Maturity Model, to guide communities in developing their own cybersecurity programs.



Community Engagement

INSTRUCTOR-LED. 8 hours.

This course is designed to help participants practice and refine cybersecurity skills and procedures developed independently, within a coordinated training environment. Attendees work collaboratively to enhance preparedness, response, and recovery capabilities in an All-Hazards event. Through interactive sessions and real-world scenarios, participants strengthen their ability to work as a cohesive unit, ensuring a more resilient and prepared community.



Maritime Cybersecurity Compliance Fundamentals (MGT-368)

INSTRUCTOR-LED. 8 hours

Participants will develop an understanding of how cybersecurity risks affect maritime operations, regulatory compliance and organizational readiness. Through facilitated discussion and case-based analysis, the course emphasizes cyber threat recognition, incident reporting, documentation, and coordination with designated cybersecurity personnel. The course prepares participants to support compliance activities, contribute to organizational decision-making, and maintain readiness for U.S. Coast Guard inspections, audits and real-world cyber incidents.

Cyber Incident Response & Recovery

Integration of Cybersecurity Personnel into the Emergency Operations Center for Cyber Incidents (MGT-456)

INSTRUCTOR-LED. 24 hours; 2.4 CEUs.

This course is designed to assist jurisdictions with coordinating and managing response efforts between emergency response organizations and critical infrastructure cybersecurity personnel. The course will help to ensure that traditional emergency management personnel and cybersecurity personnel recognize the importance of working together to mitigate the effects of a cyber incident. This course utilizes the Emergency Management Exercise System (EM*ES) incident simulation software.

Recovering from Cybersecurity Incidents (MGT-465)

INSTRUCTOR-LED. 16 hours; 1.6 CEUs.

This course provides guidance to a jurisdiction on the actions necessary to effectively recover from a cybersecurity attack. It discusses the pre- and post-incident programmatic activities needed for short-term and long-term recovery, and bridges the different worlds of information technology and emergency management.

CYBER INCIDENT RESPONSE & RECOVERY Courses >>



Cyber Incident Response & Recovery



Cybersecurity Incident Response and Management (PER-371)

INSTRUCTOR-LED. 24 hours; 2.4 CEUs.

This course utilizes NIST 800-61r2 to introduce participants to the cyber incident lifecycle. By engaging with a virtual cyber range, participants will gain hands-on experience in responding to simulated real-world cyber attacks, enhancing their understanding of the critical role of information exchange during live cyber incidents. This course integrates the Incident Command System (ICS) to equip the public and private sectors with the framework, knowledge and practical skills needed to navigate and manage the full spectrum of the cyber incident lifecycle.



Developing a Cybersecurity Annex for Incident Response (MGT-367-W)

WEB-BASED. 6 hours.

This course addresses the need for a strategic-level "how to" of responding to and sharing information about cybersecurity incidents through the cyber annex vehicle. At the end of this course, participants should possess the fundamentals needed to design and develop a cyber annex for states, locals, tribes and/or territories (SLTTs). It addresses what the annex is, how it is used, and who should participate in the design, implementation and execution.



Disaster Recovery for Information Systems (AWR-176-W)

WEB-BASED. 10 hours; 1.0 CEUs; 1 hour - ACE; 1 semester hour.

This course trains business managers to respond to varying threats that might impact their organization's access to information. The course provides requisite background theory and recommended best practices needed by managers to keep their offices running during incidents of different types. Topics include disaster recovery planning; guides for implementing and managing disaster recovery plans; a discussion of technical vulnerabilities; and an examination of legal issues.

Incident Response for Municipal, Police, Fire & EMS IT Personnel (AWR-389-W)

WEB-BASED. 2 hours; .2 CEUs.

The course introduces the basics of the incident response process to the Information Technology personnel in Police, Fire or EMS departments. The content of the course will include: cyber incidents in Police, Fire, EMS and IT departments, and developing a response plan to cyber incidents.

Introduction to Cyber Incident Management (AWR-169-W)

WEB-BASED. 9 hours; 1.0 CEUs; 1 hour - ACE; 1 semester hour.

This course provides practical guidelines on responding to incidents effectively and efficiently as part of an incident response program. Primary topics include detecting, analyzing, priortizing and handling cyber incidents. Real-world examples and scenarios to help provide knowledge, understanding and capacity for effective cyber incident analysis and response.

Network Traffic Analysis (PER-418)

INSTRUCTOR-LED. 24 hours.

This course will train students to conduct traffic analysis on their internal networks by doing a “deep-dive” into network traffic analysis using Wireshark and other tools to identify regular and anomalous network traffic. It will teach techniques necessary to identify network attacks by context and type.

Cyber Threat Hunting (PER-366)

INSTRUCTOR-LED. 32 hours.

COMING SOON

Using a blended learning approach, this course provides technical personnel with a strategy to proactively recognize and mitigate adversarial cyber events. Participants will have an increased understanding of the cyber threat landscape and establish a methodology to hunt for relevant system compromises to eliminate or limit their damage. Through skills-based labs, they will use tools to gather cyber intel and sift through logs, network traffic, and memory to identify and triage potential threats.

KEY

Web-Based Course

Instructor-Led Course

COMING SOON

Courses Under Development

Information Technology

End User

Management/ Leadership



Technical

Comprehensive Cybersecurity Defense (PER-256)

INSTRUCTOR-LED. 32 hours.

A basic-level course designed for technical personnel who monitor and protect our nation's critical cyber infrastructure. The course introduces students to cyber-defense tools that will assist in monitoring their computer networks and implementing cybersecurity measures to prevent or greatly reduce the risk of a cyber-based attack. This course integrates hands-on computer lab applications to maximize the student's learning experience.

Cybersecurity First Responder (PER-257)

INSTRUCTOR-LED. 32 hours.

An intermediate-level course designed for technical personnel who are first responders to any type of cyber-based attack. Includes the use of response tools against real world simulated cyber-attacks. Students learn the steps of an incident response to include incident assessment, detection and analysis, and containing, eradicating and recovering processes from a system or network-based attack.

Cybersecurity Proactive Defense (PER-377)

INSTRUCTOR-LED. 32 hours.

An advanced-level course for technical personel who monitor and protect critical cyber infrastructure. It uses hands-on computer lab applications to simulate advanced attack vectors, sequential and escalating attack steps, and attack execution. Learn penetration testing skills, defense analysis techniques, and real-time response and threat mitigation steps.

Cybersecurity Resiliency in Industrial Control Systems (PER-398)

INSTRUCTOR-LED. 8 hours.

This course will review the Internet of Things vulnerabilities within Operational Technology and Supervisory Control and Data Acquisition systems, methods of detecting and responding to cyber attacks in the systems, and actions that can be taken by non-technical personnel to mitigate or minimize the effects of cyber attacks.

Malware Prevention, Discovery and Recovery (PER-382)

INSTRUCTOR-LED. 32 hours.

An intermediate-level course designed for technical personnel who monitor and protect critical cyber infrastructure. Learn how to recognize, identify, and analyze malware; the remediation process to eliminate the malware; and proper procedures to recover from the attack and regain network connectivity.

Cyber Identity and Authentication (AWR-384-W)

WEB-BASED. 6 hours; .6 CEUs.

This course addresses different forms of authentication, such as two-factor, multi-factor and other protections addressing identity compromise. Designed for public and private personnel at all levels of government, law enforcement, the private sector and other stakeholders, this course provides a broad-base of knowledge connecting the underlying concepts of digital identity to how people, devices and systems are authorized to access digital resources and services.

TECHNICAL TRAINING Courses >>

KEY

Web-Based Course

Instructor-Led Course

Courses Under Development

Information Technology

End User

Management/ Leadership

Technical

Cybersecurity Fundamentals (AWR-418-W)

WEB-BASED. 4 hours.

An introductory level course for new and transitioning Information Technology professionals. Students learn preferred network topologies and the uses of Intrusion Detection/Prevention systems; the use and maintenance of firewalls and anti-virus software; to recognize various types of network-based attacks; to recognize social engineering attacks; the importance of establishing policies, and disaster planning.

Digital Forensics Basics (AWR-139-W)

WEB-BASED. 10 hours; 1.0 CEUs; 1 hour - ACE; 1 semester hour.

This course covers investigative methods and standards for the acquisition, extraction, preservation, analysis and deposition of digital evidence from storage devices. It offers a wide array of forensics situations that are applicable to the real world. Participants will learn how to find traces of illegal or illicit activities left on digital media and devices with computer forensics tools and manual techniques and how to recover data intentionally hidden or encrypted by perpetrators.

End-User Security and Privacy (AWR-300-W)

WEB-BASED. 4 hours.

Focused on the end-user's perspective; in particular, various security-related challenges and their impact on data privacy. Includes content concerning online content providers on access rights, unintentional data sharing, mobile apps and being compliant to a NIAP Protection Profile (PP). Addtionally, this course equips end-users to adequately configure firewalls, routers, switches and implement network segmentation. It provides instructions for using device and file locking mechanisms for personal computers and mobile devices; how to set up different types of user accounts; and how to secure cyber-enabled devices on smart home networks.

Examining Advanced Persistent Threats (AWR-403-W)

WEB-BASED. 4 hours; .4 CEUs.

Learn best practices that can assist in protecting against advanced persistent threats. This course provides a broad base of knowledge focused on how to prepare for, respond to and recover from the impacts of advanced cyber-attacks that exploit targeted victims. At the end of this course, participants should possess a fundamental understanding of the most common attack path for various advanced persistent threats (APTs).

Information Risk Management (AWR-177-W)

WEB-BASED. 5 hours; 1.3 CEUs; 1 semester hour.

This course addresses topics related to information assets, identifying risks, and management processes. Receive training on information risk-related tools and technologies for better understanding of potential threats and vulnerabilities in online business. Learn best practices and how to apply levels of security measures.

Information Security Basics (AWR-173-W)

WEB-BASED. 13 hrs; 1.3 CEUs; 1 hour - ACE; 1 semester hour.

This course provides entry/mid-level IT staff a technical overview of information security, focusing on the knowledge to identify and stop various cyber threats. General concepts and topics covered include TCP/IP protocol, introductory network security, introductory operating system security, and basic cryptography.

Network Assurance (AWR-138-W)

WEB-BASED. 6 hours; .5 CEUs; 1 semester hour.

This course covers secure network practices to protect networked systems against attacks and exploits. Topics include authentication, authorization, and accounting (AAA), as well as firewalls, intrusion detection/prevention, common cryptographic ciphers, server and client security, and secure policy generation.

Secure Software (AWR-178-W)

WEB-BASED. 9 hours; 1 semester hour.

This course teaches programming practices used to secure applications against attacks and exploits. Fundamental concepts and topics covered include secure software development, defensive programming techniques, secure design and testing, and secure development methodologies.

Zero Trust: Identity and Access Management (AWR-351-W)

WEB-BASED. 5 hours.

This course will address concepts related to Zero Trust and Access Control. Students will learn different forms of access control and their usages in practice, the concept of zero trust, the shift from perimeter-based security to Zero Trust, and Zero Trust implementation.

Artificial Intelligence (AI) Security (PER-341)

INSTRUCTOR-LED. 24 hours.

COMING SOON

This course will explore the ever-changing ChatGPT ecosystem, which is an interactive Artificial Intelligence (AI) Machine Learning (ML) system that generates human-readable text to interact with us. ChatGPT can be a valuable tool for organizations and individuals who want to find and fix security vulnerabilities. However, in the wrong hands, the service can become a dangerous tool for hackers.

Cybersecurity Threats and Systems in Maritime Environments

INSTRUCTOR-LED. 16 hours.

COMING SOON

The course emphasizes execution-level interaction with maritime IT and OT systems and focuses on cybersecurity conditions that may arise during routine operations and abnormal events. Instruction is designed to be accessible to non-technical maritime personnel and emphasizes recognizing cyber-relevant conditions, assessing potential operational impacts, and determining appropriate response or escalation actions rather than performing technical system configuration or analysis.

Cyber Threat Information Sharing



Community Cybersecurity Information Sharing Integration (MGT-478)

INSTRUCTOR-LED. 16 hours.

This course will show SLTTs how to integrate cybersecurity information sharing into their community programs. Learn to strategically design and implement a cybersecurity information sharing program for the state, territory, tribe, jurisdiction or region. This includes governance; creating public/private partnerships; and coordinating efforts to prevent, mitigate and counter attacks for a community.

Organizational Cybersecurity Information Sharing (MGT-473)

INSTRUCTOR-LED. 16 hours.

This course introduces fundamental cyber information sharing concepts that can be incorporated into a cybersecurity program for both inside and outside an agency or organization. It introduces the purpose and value of information sharing and how sharing can assist with cyber incident preparedness and response before, during and after a cyber incident occurs.

CYBER THREAT INFORMATION SHARING TRAINING Courses >>

Cyber Threat Information Sharing



Cyber Threat Intelligence (PER-412)

INSTRUCTOR-LED. 16 hours.



This course introduces the information analysis process and how an organization can use it to identify, define and mitigate cybersecurity threats. Participants will gain a general understanding of the tools and processes needed for an analysis team to create cybersecurity information and intelligence within their organization. It establishes a framework for an analytical process; how shared analysis can provide actionable information, reduce uncertainty and reduce risk to enable decision makers.



Establishing an Information Sharing and Analysis Organization (MGT-366-W)



WEB-BASED. 8 hours; .8 CEUs.

This course will assist communities to establish an Information Sharing and Analysis Organization (ISAO). The course will introduce the value proposition of creating an ISAO and provide considerations to joining an existing ISAO. It will closely follow the guidance provided by the ISAO Standards Organization (ISAO SO), whose mission is to “improve the nation’s cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices”.



Introduction to ISAOs (AWR-398-W)



WEB-BASED. 2 hours; .2 CEUs.

This course is designed to introduce the basics of the cybersecurity information sharing processes. Participants will have an increased knowledge of cyber security information sharing and an understanding of the steps taken to join or establish an ISAO/ISAC.

Target Audiences

The National Cybersecurity Preparedness Consortium (NCPC) emphasizes cybersecurity as being the responsiblity of the “whole community”. This includes public and private sectors, as well as any individual within the community.

The NCPC courses target three primary audiences within your community:



Leadership/Management

Any leader, including non-technical, is ideal for this type of course. If a finance/accounting leader could take the class, it applies to leadership.



Information Technology (IT)

Includes anyone with a technology role. In some organizations, this may only apply to technology/ cybersecurity leaders.



End User

Any person within an organization or community. Likely, no prerequisites are required to take a course designed for end-users.

Non-technical professionals or specialist. For example, emergency manager, risk managers, compliance and auditors.

"Our cyber infrastructure is every bit as important as our roads and bridges. It's important to our economy. It's important to protecting human life, and we need to make sure we have a modern and resilient cyber infrastructure."

~ Rep. Jim Langevin,
Co-Chair of the Congressional
Cybersecurity Caucus

Thank you for your interest in the National Cybersecurity Preparedness Consortium (NCPC) courses. All courses are certified and administered through the DHS Federal Emergency Management Agency (FEMA). Thanks to FEMA, these cybersecurity training courses are available at no cost.

To register for NCPC web-based and instructor-led courses, contact your state's Homeland Security Training Office. More information on how to register for courses is available on NationalCPC.org.