NCPC
National Cybersecurity Preparedness Consortium

Become a **PARTNERING HOST** in your Community

CYBERSECURITY TRAINING

Designed for States, Local Governments, Tribes, and Territories

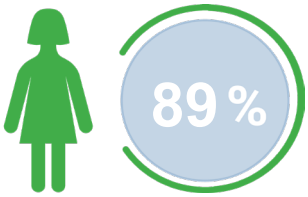
CONGRESSIONALLY FUNDED

OUR IMPACT

The National Cybersecurity Preparedness Consortium (NCPC) has achieved significant milestones in the development, certification and delivery of cybersecurity training in partnership with the Department of Homeland Security's Federal Emergency Management Agency (FEMA).

There are currently **51 courses available**, with 15 in development.

90 percent of SLTT participants have used the concepts learned on the job



89 percent of SLTT participants agreed that they're better prepared after taking the training

151,705 Participants

OUR MISSION

To help State, Local, Tribe and Territory (SLTT) governments establish viable and sustainable programs to prevent, detect, respond to, and recover from cyber attacks.

TRAINING CATEGORIES

The NCPC provides FEMA certified, cybersecurity related training, exercises and technical assistance to SLTT communities. This training is applicable to all sectors.

Whether you are a leader, IT practitioner or end user, the NCPC has training for you in the following categories:

- AWARENESS
- COORDINATION & PLANNING
- CYBER THREAT INFORMATION SHARING
- TECHNICAL
- CYBER INCIDENT RESPONSE & RECOVERY

IN-PERSON, WEB-BASED and VIRTUAL COURSES AVAILABLE

FEMA

NCPC courses are no cost to participants. These courses are certified and administered through DHS/FEMA.

NationalCPC.org

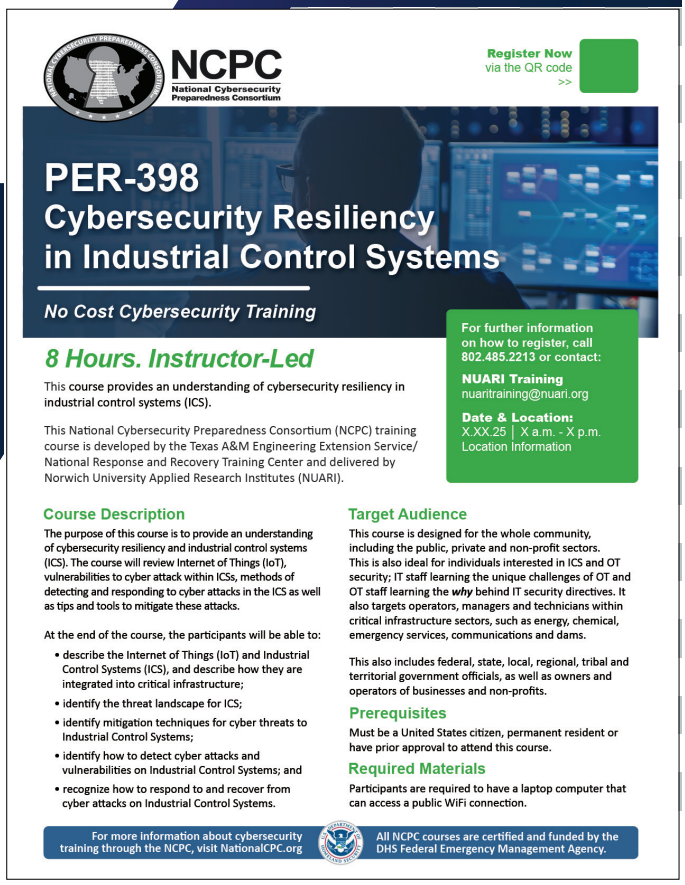
NCPC
National Cybersecurity Preparedness Consortium

Did you know?

Each course comes with a custom promotional flyer to help recruit participants.

The flyers include an easy QR Code for course registration, along with information on its virtual or in-person location and contact information.

All Deliveries are NO COST



NCPC
National Cybersecurity Preparedness Consortium

Register Now via the QR code >>

PER-398
Cybersecurity Resiliency in Industrial Control Systems

No Cost Cybersecurity Training

For further information on how to register, call 802.485.2213 or contact:

NUARI Training
nuaritraining@nuari.org

Date & Location:
X.XX.25 | X a.m. - X p.m.
Location Information

8 Hours. Instructor-Led

This course provides an understanding of cybersecurity resiliency in industrial control systems (ICS).

This National Cybersecurity Preparedness Consortium (NCPC) training course is developed by the Texas A&M Engineering Extension Service/ National Response and Recovery Training Center and delivered by Norwich University Applied Research Institutes (NUARI).

Course Description

The purpose of this course is to provide an understanding of cybersecurity resiliency and industrial control systems (ICS). The course will review Internet of Things (IoT), vulnerabilities to cyber attack within ICSs, methods of detecting and responding to cyber attacks in the ICS as well as tips and tools to mitigate these attacks.

At the end of the course, the participants will be able to:

- describe the Internet of Things (IoT) and Industrial Control Systems (ICS), and describe how they are integrated into critical infrastructure;
- identify the threat landscape for ICS;
- identify mitigation techniques for cyber threats to Industrial Control Systems;
- identify how to detect cyber attacks and vulnerabilities on Industrial Control Systems; and
- recognize how to respond to and recover from cyber attacks on Industrial Control Systems.

Target Audience

This course is designed for the whole community, including the public, private and non-profit sectors. This is also ideal for individuals interested in ICS and OT security; IT staff learning the unique challenges of OT and OT staff learning the ***why*** behind IT security directives. It also targets operators, managers and technicians within critical infrastructure sectors, such as energy, chemical, emergency services, communications and dams.

This also includes federal, state, local, regional, tribal and territorial government officials, as well as owners and operators of businesses and non-profits.

Prerequisites

Must be a United States citizen, permanent resident or have prior approval to attend this course.

Required Materials

Participants are required to have a laptop computer that can access a public WiFi connection.

For more information about cybersecurity training through the NCPC, visit NationalCPC.org

All NCPC courses are certified and funded by the DHS Federal Emergency Management Agency.

Partnering with NCPC as a host site offers your organization the opportunity to support accessible, hands-on cybersecurity training for public and private sector professionals. Hosting a course brings valuable resources to your region while contributing to a broader mission of enhancing national cyber preparedness.

Partnering Hosts:

- Provide classroom facilities to support students
- Utilize your community networks and relationships to fill seats
- Have the first opportunity to be pilot sites for new courses

NCPC Provides:

- FEMA-certified course materials
- Quality cybersecurity instructors
- Registration support

Schedule a delivery today!

NCPC is booking training dates across the U.S. for 2026 and 2027 now.

Contact us to reserve your preferred dates!

nuaritraining@nuari.org

All NCPC courses are certified and administered through DHS/FEMA.

NCPC
National Cybersecurity Preparedness Consortium

NCPC
National Cybersecurity Preparedness Consortium

Contact NUARI to schedule your next NCPC course delivery!

NCPC CYBERSECURITY COURSES SCHEDULED & DELIVERED THROUGH Norwich University Applied Research Institutes (NUARI)

AWR-427 Cybercrime Insight and Introduction to Digital Evidence Identification

8 Hours. Instructor-Led (In-Person Only).

This course introduces 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 how to incorporate the evidence into an investigation.

Participants will be introduced to the fundamentals of computer networks and internet technologies, as well as learn how to identify hardware, software and other digital devices that often contain evidence used in criminal investigations. The focus will be on teaching students how to recognize that an incident has occurred and who to contact about gathering evidence.

Target Audience: Police officers, security professionals, federal agents, emergency management personnel, investigators and detectives.

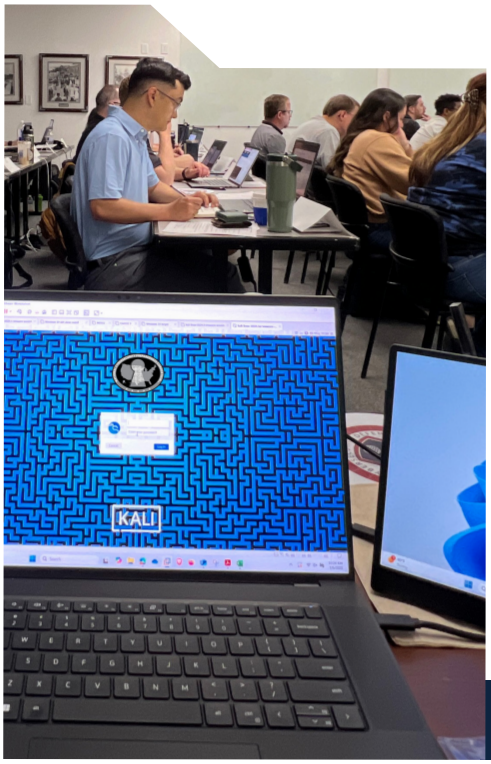
AWR-428 Practical Internet of Things (IoT) Security

8 Hours. Instructor-Led (In-Person Only).

This classroom-based activity is designed to introduce students to identify and describe the components of an IoT system and associated security concerns. The course will cover the elements of an IoT system including programmable logic controllers, sensors and network interfaces. Topics will include PLC functions and programming, common IoT network protocols and security concerns related to IoT systems.

Lecture and exercises will culminate in a laboratory experience where teams of students will build an IoT system and examine security considerations, vulnerabilities, and threats. No prior programming experience is required.

Target Audience: Individuals working in an IT or critical infrastructure provider role where IoT may be installed or employed.



PER-398 Cybersecurity Resiliency in Industrial Control Systems

8 Hours. Instructor-Led (In-Person Only).

The purpose of this course is to provide an understanding of cybersecurity resiliency and industrial control systems (ICS). The course will review Internet of Things (IoT), vulnerabilities to cyber attack within ICSs, methods of detecting and responding to cyber attacks in the ICS as well as tips and tools to mitigate these attacks.

Target Audience: Whole community; public, private and non-profit, individuals interested in ICS and OT security; IT staff learning the unique challenges of OT, and OT staff learning the why behind IT security directives; State, local, tribal and territorial government officials; Owners and operators of businesses and non-profits; Risk management personnel; Critical infrastructure sectors (e.g., Energy, Chemical, Emergency Services, Communications, Dams).

AWR-383 Cybersecurity Risk Awareness for Officials and Senior Management

4 Hours. Instructor-Led (In-Person Only).

This non-technical 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. It is designed to help officials and senior management work more effectively with their Information Technology (IT) departments to mitigate cyber threats.

Upon successful completion of the course, participants will have a better understanding of the cybersecurity risks that their jurisdiction or organization faces and how to work with their IT teams and other departments to mitigate those risks.

Target Audience: Any person who works for a public or private organization in an executive or upper management capacity. This includes elected officials; city managers; chief information officers; risk managers; emergency management coordinators; jurisdictional department heads; and directors of critical infrastructure.

AWR-432 Integrating Cyber Hazard Response into Exercise Planning

4 Hours. Instructor-Led (In-Person or Virtual).

This course is designed to teach exercise planners the importance of incorporating cyber into all hazard emergency management. While most exercise planners know cyber-hazards exists, they may have not been taught how to incorporate those hazards into their exercise planning. Furthermore, exercise planners may not know the extent to which cyber hazards impact critical infrastructure.

This course will ensure exercise planners are aware of the hazards related to cyber-enabled threats and how to address those hazards within their exercises.

Target Audience: Exercise planners; EP team leaders; THIRA managers; emergency management personnel; and cyber plan and policy managers.

AWR-301 Cybersecurity for Educational Leaders

8 Hours. Instructor-Led (In-Person Only).

This non-technical course is focused on educational institutions to assist them in addressing cybersecurity threats. Educational institutions of all sizes (including universities, colleges and K-12 school districts) 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 course introduces key cybersecurity concerns for leaders and fosters discussions to build strategies of cybersecurity preparedness to ensure adequate resources are considered to meet data privacy and cybersecurity needs.

Target Audience: University and college leadership and mid-level managers/administrators and K-12 School Administrators; school security staff; and those that determine a school's mission and purpose.

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

4 Hours. Instructor-Led (In-Person or Virtual).

This course enables leaders to define and assess business risks related to cybersecurity. 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 methods to calculate risk. Instruction includes discussion of risk management frameworks outside of NIST (e.g., OCTAVE FORTE) and Factor Analysis of Information Risk (FAIR) for risk assessment. It also teaches leaders methods to identify, define and measure risk to their organization from multi-faceted threats incorporating cyber, physical and other means. They begin with a module on critical thinking to open their minds to later modules, which discuss concepts outside standard risk management frameworks. The final modules familiarize students with common language taxonomies, various risk management frameworks and FAIR.

Target Audience: Business, IT, and OT leadership and operations staff at varying experience levels, with a focus on exposing Risk Management and Assessment thought processes to resource-constrained SLTT populations.

AWR-388-W Cyber Security Awareness for Municipal, Police, Fire and EMS IT Personnel

2 Hours. Web-based Training (Self-Paced)

This course covers basic cyber awareness for Municipal, Police, Fire and EMS Information Technology personnel. Participants will have an increased knowledge of threats specific to their jurisdiction and an understanding of the processes and procedures needed to develop a cyber-awareness program. This course will focus on the steps involved in being aware of cyber threats and effectively communicating the processes and procedures to protect users against common cyber threats.

Target Audience: This course is designed for Information Technology Support Personnel and technically proficient mid-level management in the public sector. The course is not designed for firefighters, police officers or EMTs.

AWR-389-W Incident Response for Municipal, Police, Fire and EMS Information Technology Personnel

2 Hours. Web-based Training (Self-Paced)

This course is the second training in a two-part course. It is intended to introduce the basics of the incident response process to the Information Technology personnel in Police, Fire or EMS departments. This web-based course focuses on the steps involved in being aware of common cyber incidents, as well as steps in developing an incident response plan.

Target Audience: This course is designed for Information Technology Support Personnel and technically proficient mid-level management in the public sector. The course is not designed for firefighters, police officers or EMTs.

Piloting now! These courses are in development as part of the FEMA certification process - schedule now for priority access, be among the first to attend, and help shape the final content with your feedback.

Maritime Cybersecurity Compliance Fundamentals

8 Hours. Instructor-Led (Virtual Only).

This course provides management-level instruction on maritime cybersecurity compliance requirements for personnel with responsibilities involving Information Technology (IT) and Operational Technology (OT) systems within the domain of the Marine Transportation System (MTS).

Target Audience: Maritime personnel with management, supervisory, or operational responsibilities involving access to IT or OT systems across vessels, port facilities, or OCS operations.

Cybersecurity Threats and Systems in Maritime Environments

16 Hours. Instructor-Led (In-Person Only).

This course is to prepare maritime personnel to perform cybersecurity-related tasks during both routine operations and abnormal events in alignment with regulatory and organizational requirements.

Target Audience: Maritime personnel responsible for operating, maintaining, or monitoring IT and/or OT systems supporting vessel, facility, and Outer Continental Shelf (OCS) operations.

Developing a Resilient Cybersecure Community

8 Hours. Instructor-Led (In-Person Only).

The course will work within the National Preparedness System's preparedness cycle, focusing on Plan, Train, and Exercise. At the end of this course, participants will be able to measure their current preparedness, identify gaps, and experience role-playing through a community-level response scenario of an event that has either a cyber root cause or a cyber-attack that degrades response. The result of this training would be a more aware, resilient, cybersecure community.

Target Audience: The primary audience that should attend this interactive, cybersecurity-focused resilience and response training are leaders or managers, their teams, and response partners who perform planning, training, or exercising critical and business functions within their community or organization as part of its Community Lifelines.

PER-388 Cybersecurity in a Resource Constrained Environment for Public and Rural Utilities

16 Hours. Instructor-Led (In-Person Only).

The course introduces foundational cybersecurity principles in the context of community and critical infrastructure protection. Through classroom instruction, guided labs, and applied exercises, participants explore common threats, examine open-source tools for monitoring networks and systems, and review key cybersecurity standards and policies. Using these concepts, participants will develop a practical outline for a cybersecurity program that reflects their organization's resources and operational realities, incorporating both technical and administrative controls to support ongoing program development and implementation.

Target Audience: Designed for decision-makers and technology professionals supporting community organizations and critical infrastructure sectors.

> "This was, by far, one of the best, if not the best class I've attended in years. The instructors were very engaging throughout the presentation and inclusive in every way. I particularly enjoyed the informal Q&As and polls to check knowledge and understanding. Kudos to the team!"
>
> *~ Participant Testimonial*

OUR PARTNERS

The National Cybersecurity Preparedness Consortium (NCPC consists of five partner universities.

Criminal Justice Institute (CJI), University of Arkansas System

CJI, established in 1994, has competencies working with law enforcement and school safety. Their robust cybersecurity technical competencies in organizational critical infrastructure directly influence relevant and timely hands-on training for technical roles.

Center for Infrastructure Assurance & Security (CIAS), The University of Texas at San Antonio

Since 2002, the CIAS has focused on whole community cybersecurity programs, achieving extensive experience in cybersecurity exercises, game development, information sharing, and cyber defense competitions. The CIAS also provides a unique, cloud-based platform enabling hands-on labs and Cyber Range capabilities, for immersive and scalable NCPC training experiences. The director of the CIAS, Natalie Sjelin, is chair of the NCPC.

The Texas A&M Engineering Extension Service (TEEX), National Emergency Response & Recovery Training Center (NERRTC)

Since 1998, TEEX/NERRTC has worked with first responder/emergency management personnel, training over 1 million nationally. They bring experience on how emergency responders and IT professionals can collaboratively address the cybersecurity risks jurisdictions face. TEEX/NERRTC also provides a centralized function, hosting all NCPC web-based courses on their Learning Management System.

Center for Information Assurance (CfIA), University of Memphis

The CfIA is instrumental in performing advanced cybersecurity research and developing timely, forward-thinking cybersecurity strategies and training. These efforts are integrated into NCPC web-based offerings—such as zero trust architectures, mobile device security, smart-grid security, and more—to help educate technologists and end users about cyber-attacks and mitigation techniques.

Norwich University Applied Research Institutes (NUARI)

NUARI's experience and relationships with the Department of Defense and the financial sectors adds additional community perspectives to NCPC training. NUARI's expertise with cybersecurity exercises and the creation of the DECIDE® platform for live cybersecurity exercises strengthens the NCPC strategies, training and planning for SLTTs. Their innovative approach to developing cybersecurity tools also helps the NCPC address cybersecurity preparedness.