Your Guide
to Community
Cyber Security

TRAINING and EXERCISE COURSES

FEMA

NationalCPC.org

TABLE of CONTENTS

FEMA

Mission Statement

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.

Purpose

The purpose of the consortium is to provide assistance to states and communities trying to develop viable and sustainable cybersecurity programs. This includes both the development and delivery of cybersecurity training, the development and delivery of cybersecurity exercises, and the use of competitions and workshops to encourage both interest in cybersecurity as well as consideration by individuals of cybersecurity as a career choice.

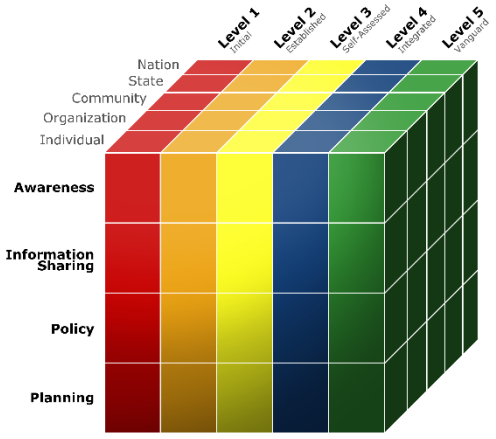
Using the Community Cyber Security Maturity Model (CCSMM) as a basis from which to work, the consortium collectively works with states and communities as they progress through the model. An important aspect of the model is that it does not address IT professionals alone; it involves all individuals at the appropriate time in the maturity of the community. For everyone, it begins with simple awareness of cybersecurity as an issue, progresses through a point where the organization can conduct its own activities and assessments, and then finally to a point that it can become part of the vanguard in the state to help others as well.

Research, Training, and Technical Assistance Philosophy

Utilizing CCSMM as its core rubric, the NCPC endeavors to provide a well-coordinated, focused and threat-responsive long-term national capability based on applicable DHS doctrine in support of the National Preparedness Goal. In addition, the NCPC will ensure its continued relevance and value to national preparedness efforts through its customer-focused contact and communication and by correlating its comprehensive efforts to the annual *National Preparedness Report*.

The Model

The consortium is organized around the CCSMM. This model is based on over a decade of experience with states and communities trying to develop viable and sustainable cybersecurity programs. It addresses three main requirements:



- A “yardstick” to allow a state or community to measure their current level of cybersecurity maturity. They can determine where they are in the model.
- A “roadmap” so a state or community can know what they need to do in order to advance the state of their cyber preparedness. There are clear steps for them to improve their security posture.
- A common “point of reference” so individuals from different states and communities can discuss their programs and the issues they face from a common perspective.

Experience

As early as 2004, in partnership with DHS/FEMA, the individual members of the NCPC have developed and delivered DHS/FEMA certified *online* and *face-to-face* training courses to an array of states, counties, local jurisdictions, and critical infrastructure components nationwide addressing cybersecurity and cyber terrorism concerns.

As of September 2018, members of the Consortium have trained more than 82,730 participants:

- CIAS – 7,848 trained
- CJI – 5,562 trained
- CfIA – 4,677 trained
- NUARI – 1,210 trained
- NERRTC – 63,433 trained

NCPC Membership

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

The CIAS developed the Community Cyber Security Maturity Model (CCSMM) upon which the NCPC is based. The CIAS has worked with states and communities to conduct cybersecurity training, exercises, workshops, and seminars for over a decade. It has participated in cybersecurity exercises at the sector and national level as well. The CIAS developed six courses that have been evaluated and accepted as part of the official DHS/FEMA National Training and Education Division (NTED) catalog.

The Criminal Justice Institute (CJI), University of Arkansas System

CJI's Cyberterrorism Defense Initiative (CDI) is a national counter-cyberterrorism training program for technical personnel who monitor and protect our nation's critical cyber infrastructure. Courses are delivered utilizing blended learning that combines instructor-led classroom lecture with hands-on computer lab applications by use of a mobile computer training lab. The training enhances the abilities of our nation's cyber first responders to prevent, protect against, respond to or recover from any type of cyber-based attack against our nation's critical cyber infrastructure. Since 2004 CJI has developed six technical level courses that have been delivered to technical personnel in 33 states and one U.S. territory.

The University of Memphis, Center for Information Assurance (CfIA)

The CfIA at the University of Memphis is at the forefront in the research, education, and outreach of Information Assurance (IA) in the Mid-South region. The center represents the collaboration of multiple academic disciplines, in partnership with community colleges, focusing on cybersecurity-related topics. It provides research, education, and awareness in the critical realm of cybersecurity and IA. The University of Memphis currently offers two graduate certificate programs in IA, one through the Department of Computer Science, and the other one, Business Information Assurance, is offered through the Department of Management Information Systems. The center was involved in the development of a multi-track, multi-level, online cybersecurity training program, including 10 web-based DHS/FEMA certified courses. Faculty involved with CfIA have engaged in multi-disciplinary research activities in

cybersecurity, spearheading collaborative research efforts in areas that include secure health informatics, privacy-preserving mobile health, smart grid security, and secure supply chain.

Norwich University Applied Research Institutes (NUARI)

NUARI draws on its long history as a leader in cybersecurity research and training to provide curricula and mission support services across all industries and sectors. Federally chartered under legislation sponsored by Senator Patrick Leahy in 2002, NUARI is a 501(c)(3) nonprofit corporation that is funded in part through the Department of Homeland Security and The Department of Defense.

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

TEEX/NERRTC provides tailored, specialized training in the areas of cybersecurity, crisis communications, disaster management for executives and elected officials, hazardous materials, health and medical services, incident management, infrastructure protection, search and rescue, threat and risk assessment, and training gap analysis. This training enhances the capacity of emergency responders to prevent, protect against, respond to, recover from, and mitigate against incidents of national significance, including all-hazards events and terrorism. TEEX/NERRTC delivers cybersecurity training both online and in the classroom. The online training is designed for individuals to increase awareness as general users, IT technical users or business management users. The classroom training for responders is delivered in a state or local jurisdiction and focuses on integrating cybersecurity into a community's Emergency Operations Center or exercise planning.

CJI – University of Arkansas System

POC: William Byrd | CyberTerrorismCenter.org | (501) 570-8084 | wcbyrd@cji.edu

Comprehensive Cyberterrorism Defense (CCD) (PER-256) **(Length – 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 them in monitoring their computer networks and implementing cyber-security 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.

Cyberterrorism First Responder (CFR) (PER-257) **(Length – 32 hours)**
An intermediate-level course designed for technical personnel who are first responders to any type of cyber-based attack against our nation's critical cyber infrastructure. Blended learning methods are utilized, to include a balance of classroom lecture, hands-on laboratory exercises, and the use of cyberterrorism response tools against real world simulated cyber-attacks. Students learn the proper steps of an incident response to include incident assessment, detection and analysis, and the containing, eradicating, and recovering process from a system or network-based attack.

NERRTC – Texas A&M Engineering Extension Service

POC: Knowledge Engineering | TEEX.org/Cyber | (800) 541-7149 | ke@teex.tamu.edu

Essentials of Community Cybersecurity (AWR-136) **(Length – 4 hours; .4 CEUs)**
This discussion-based, non-technical course originally developed by the CIAS is an introduction to cybersecurity provides individuals, community leaders, and first responders with information on how cyber attacks can impact, prevent, and/or stop operations and emergency responses in a community. The course also provides a cursory introduction to cybersecurity vulnerabilities, risks, threats, and countermeasures. It explains vulnerabilities of computer systems and networks and how these vulnerabilities can affect communities, organizations, and daily workplace operations. The course introduces actions communities can take in establishing a cybersecurity program. The course provides participants with an awareness of issues. It gives an overview of threats and vulnerabilities, without going into too many details, to highlight the potential impact a cyber attack could have. Participants discuss some of the fundamental activities needed to develop a cybersecurity program, without addressing the technical details of how to secure critical infrastructures. The course introduces the Community Cybersecurity Maturity Model (CCSMM) as a framework for understanding community cybersecurity and offers a brief introduction to low-cost or no-cost approaches to securing a community against cybersecurity threats and attacks. The course sets the stage for further efforts in which a community can build a cybersecurity program.

Community Preparedness for Cyber Incidents (MGT-384) **(Length – 12 hours; 1.2 CEUs)**
This two-day non-technical course is designed to provide organizations and communities with strategies and processes to increase cyber resilience. During this 12-hour course, participants will analyze cyber threats and initial and cascading impacts of cyber 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.

Community Cyber Security Exercise Planning (MGT-385) (Length – 12 hours; 1.2 CEUs)

This two-day non-technical course is designed to introduce cybersecurity to exercise planners to help them recognize the nature and reach of cyber, so they can better help their communities prevent, detect, respond to, and recover from cyber incidents. Participants will recognize how cybersecurity can be incorporated into exercises in a meaningful way. Participants will be introduced to cyber topics and how cybersecurity can impact the business operations of an organization and community. Lecture and activities will explore objectives, players, cyber injects and challenges to incorporating cyber into exercises. Participants will be exposed to many possible injects and scenarios that can be used in an exercise. Participants will begin development of a community cybersecurity tabletop exercise. The Community Cybersecurity Maturity Model will be used to examine the contribution of exercises to a community's overall cybersecurity posture. This course teaches planning personnel how to include cybersecurity components in their regular planning process. Participants will be given the opportunity to plan cybersecurity components for future community cybersecurity exercises.

Physical and Cybersecurity for Critical Infrastructure (MGT-452) (Length – 8 hours; .8 CEUs)

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. 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, and explore resources that can be applied to improve security within an organization, business, or government entity.

Integration of Cybersecurity Personnel into the EOC for Cyber Incidents (MGT-456)

(Length – 24 hours; 2.4 CEUs)

The course is designed to assist jurisdictions with coordinating and managing response efforts between emergency response organizations and critical infrastructure cybersecurity personnel, necessary as a result of a cyber incident. 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 which provides many features that resemble or imitate actual incident management systems.

Cybersecurity Incident Response for IT Personnel (PER-371) (Length – 24 hours)

The Cybersecurity Incident Response for IT Personnel course is designed to address the gap in specific technical skills needed for an effective cyber response. This course will also help improve the limited availability of targeted hands-on IT and security training focused on cyber-attacks. This training focuses on government and private sector technical personnel who have intermediate and advanced knowledge of network operations and/or the responsibility for network security.

Recovering from Cybersecurity Incidents (MGT-465) (Length – 16 hours)

The Recovering from Cybersecurity Incidents course is designed to provide 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. The course bridges the different worlds of information technology and emergency management. This training is particularly pertinent to IT management, emergency management personnel, as well as any other government, critical infrastructure or private sector personnel who has the responsibility for recovering after a cyber incident. This course is intended to be delivered across the country to jurisdictions at all response levels: local, state, tribal, territorial, as well as private industry.

CIAS – University of Texas at San Antonio

POC: Natalie Sjelin | (210) 458-2119 | cias@utsa.edu

To Access the Course: CIAS.UTSA.edu/dhs-fema-training.html

Developing a Community Cyber Security Program (AWR-353-W) **(Length – 2 hours)**

A web-based course that will enable community leaders, network/security personnel and those individuals involved in developing or maintaining plans used for and throughout the community. This course will assist participants to understand what is required to develop a coordinated, sustained, and viable community cybersecurity program. The course will introduce participants at all levels to the DHS-supported Community Cyber Security Maturity Model (CCSMM) and can be used to guide communities and states in developing their own CCSMM-consistent cybersecurity programs. Participants will be introduced to different resources that can be used for a community program.

Developing a Cybersecurity Annex for Incident Response (AWR-366-W) **(Length – 6 hours)**

This online course addresses the need for a strategic-level "how to" of responding to and sharing information about cyber security 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, who should participate in the design, implementation and execution. This course is suitable for personnel assigned to work in the jurisdiction's emergency operations center, policy makers, elected and/or appointed officials, emergency responders, IT personnel with responsibilities for identifying and responding to cyber events for SLTT government, private industry and critical infrastructure representatives.

NERRTC – Texas A&M Engineering Extension Service

TEEX.org/Cyber | (800) 541-7149 | ke@teex.tamu.edu

Network Assurance (AWR-138-W) **(Length – 5 hours; .5 CEUs)**

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.

Digital Forensics Basics (AWR-139-W) **(Length – 7 hours; .7 CEUs)**

This course explains investigative methods and standards for the acquisition, extraction, preservation, analysis, and deposition of digital evidence from storage devices. Using realistic forensics situations, learn how to find traces of illegal or illicit activities using computer forensics tools and manual techniques. Also, learn how to recover data intentionally hidden or encrypted by perpetrators.

Cyber Law and White Collar Crime (AWR-168-W) **(Length – 10 hours; 1.0 CEUs)**

This course presents the fundamentals of computer crime from a legal perspective. Various computer crimes are described and appropriate responses by first defenders and others that encounter these crimes are offered. This course covers a wide scope of legal topics related to cybercrime.

Cyber Incident Analysis and Response (AWR-169-W) (Length – 9 hours; .9 CEUs)

This course presents various incident analysis tools and techniques that support dynamic vulnerability analysis and elimination, as well as intrusion detection, attack protection, and network/resources repair. Real-world examples and scenarios will help you prepare for effective cyber incident analysis and response.

Information Security Basics (AWR-173-W) (Length – 13 hours; 1.3 CEUs)

This course provides entry and 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.

Cyber Ethics (AWR-174-W) (Length – 13 hours; 1.3 CEUs)

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.

Information Security for Everyone (AWR-175-W) (Length – 10.5 hours; 1.0 CEUs)

This course is designed to teach the principles and practices that all computer users need to keep themselves safe, both at work and at home. By presenting best practices along with a small amount of theory, trainees are taught both what to do and why to do it. Topics covered include how to secure both clean and corrupted systems, protecting your personal data, securing simple computer networks, and safe Internet usage.

Disaster Recovery for Information Systems (AWR-176-W) (Length – 10 hours; 1.0 CEUs)

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 an overview of business continuity planning; disaster recovery planning; guides for implementing and managing disaster recovery plans, a discussion of technical vulnerabilities faced by organizations, and an examination of legal issues that may confront an organization.

Information Risk Management (AWR-177-W) (Length – 13 hours; 1.3 CEUs)

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.

Secure Software (AWR-178-W) (Length – 9 hours; 0.9 CEUs)

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.

CIAS – University of Texas at San Antonio

POC: Natalie Sjelin | (210) 458-2119 | cias@utsa.edu

Information Sharing Integration **(Length – 16 hours)**
This two-day, instructor-led course is designed for upper-level management to address information sharing as an emerging national priority. Students, in both public and private sectors, will learn concepts such as who should be leading the information-sharing initiatives, what information will be shared, what services and capabilities should be included to assist in data collection and distribution of cyber threat indicators, sources of threats and more. State, Local, Tribes and Territories (SLTTs) will understand how to integrate cyber threat information sharing into their practices, as well as train students to strategically design and implement information sharing practices. This course integrates classroom lecture and hands-on computerized exercises to apply concepts.

Establishing an Information Sharing and Analysis Organization **(Length – 4 hours)**
This web-based course will assist communities of interest 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. The course 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".

CJI – University of Arkansas System

POC: William Byrd | (501) 570-8084 | wcbyrd@cji.edu

Cybersecurity Proactive Defense (CPD) **(Length – 32 hours)**
An advanced-level instructor-led course designed for technical personnel who monitor and protect our nation's critical cyber infrastructure. CPD uses hands-on computer lab applications to simulate advanced attack vectors, sequential and escalating attack steps, and hands-on attack execution. Students learn penetration testing skills, defense analysis techniques, and real-time response and threat mitigation steps.

Malware, Prevention, Discovery and Recovery (MPDR) **(Length – 32 hours)**
An intermediate-level instructor-led course designed for technical personnel who monitor and protect our nation's critical cyber infrastructure. Students 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 in a timely manner. This course integrates hands-on computer lab applications to maximize the student's learning experience.

Cyber Security Fundamentals **(Length – 4 hours)**
A web-based introductory level course designed 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, both remote and in-person; and the importance of establishing policies, and disaster planning.

CfIA – University of Memphis

POC: Carolyn Butler | (901) 678-3916 | cltrdwll@memphis.edu

Understanding Social Engineering Attacks (USEA) **(Length – 8 hours)**
This is a web-based course will educate members of the public in the general understanding and some common defense tactics that can be used to mitigate social engineering attacks. Designed for public and private personnel at all levels of government, law enforcement, the private sector and other stakeholders, USEA provides students with 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. Phishing, spear-phishing, water-holing, ransomware and other types of advanced persistent threats.

Mobile Device Security & Privacy (MSP) **(Length – 8 hours)**
This is a web-based course that will address how to conduct mobile device risk assessments through various security best practices including observation, data analysis, monitoring activities and recovery steps. Designed for public and private personnel at all levels of government, law enforcement, the private sector and other stakeholders, MSP uses scenarios to enhance a student's understanding of how ransomware can target mobile users in the form of fake antivirus software with subject lines such as "free call updates" pretending to scan for malware.

Cyber Identity and Authentication **(Length – 8 hours)**
This is a web-based course that will address different forms of authentication, such as two-factor, multi-factor and other authentication products protections addressing identity compromise. Designed for public and private personnel at all levels of government, law enforcement, the private sector and other stakeholders, CIAA 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. This course also covers "best practices" for using identity management and access control techniques and mechanisms to develop authentication standards.

Realizing Advanced Persistent Threats **(Length – 4 hours)**
This web-based course will address best practices that can be used to assist in protecting an organization against advanced persistent threats. Designed for public and private personnel at all levels of government, law enforcement, the private sector and other stakeholders, the Realizing Advanced Persistent Threats course provides a broad base of knowledge focused on how to prepare for, respond to and recover from the impacts of advanced cyberattacks that exploit targeted victims. This course also uses interactive simulations to enhance students' understanding of complex attack paths and countermeasures for various advanced persistent threats, including ransomware and Stuxnet.

NUARI – Norwich University Applied Research Institutes

POC: nuariinfo@norwich.edu | (802) 485-2213

Introduction to Basic Vulnerability Assessment Skills (AWR-368-W) **(Length – 12 hours)**
This web based introductory course is intended to help prepare learners for the technical challenges associated with conducting vulnerability assessments and/or penetration testing. The six course modules introduce the basic skills learners will need to begin mastering in order to conduct or manage vulnerability assessments. These skills range from the "soft skills" of the ethics involved in vulnerability assessments, to the more technical skills of network scanning and packet analysis. In addition, learners are provided with an introduction to a common, open source tool, Metasploit, which is used by red teams, as well as blue teams to test networks. The content covered in this course provides learners with an understanding of the skills and knowledge needed to successfully learn how to conduct assessments in future, more technical and hands-on courses.

Cyber Awareness for Municipal, Police, Fire & EMS Information Technology Personnel **(Length – 4 hours)**
This web-based course will cover 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. The participants will apply this knowledge by developing processes and procedures to integrate cyber awareness into routine operations. Participants will gain the understanding and knowledge needed to start developing and integrating cyber awareness programs in their specific jurisdictions.

Information Sharing for Municipal, Police, Fire & EMS Information Technology Personnel
(Length – 4 hours)
The web-based course is intended to introduce Information Technology Personnel working in a municipal environment to the sharing of information related to cyber threats and vulnerabilities. The course will focus on the advantages of sharing information, as well as the methodologies for developing an initial cyber information sharing plan. The participants of this course will gain an understanding of the need for an information sharing program and the requirements for a Municipal information sharing program.

Incident Response for Municipal, Police, Fire & EMS Information Technology Personnel **(Length – 4 hours)**
This web-based course is the second training in two-part course. The course is intended to introduce 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.

NERRTC – Texas A&M Engineering Extension Service

POC: Knowledge Engineering | TEEX.org/Cyber | (800) 541-7149 | ke@teex.tamu.edu

Cyber Awareness for Senior Officials **(Length – 4 hours)**
This instructor-led workshop provides a forum to discuss strategic and executive-level issues related to cybersecurity preparedness, to share proven strategies and best practices, and to enhance coordination among officials responsible for cybersecurity response and recovery. This workshop will integrate multimedia scenarios and vignettes that highlight key issues and facilitates executive-level discussion of cyber prevention, protection and

recovery. Additionally, the forum provides an opportunity to apply lessons learned from past local and national cyber hacks and breeches.

Understanding a Targeted Cyber Attack **(Length – 8 hours)**

This instructor-led course provides participants with specific information regarding targeted cyber attacks, including advanced persistent threats. This information will place them in a better position to plan and prepare for, respond to, and recover from targeted cyber attacks. This course will fill 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.

Visit Our Website for Updates
NationalCPC.org

Courses Listed On
FirstResponderTraining.gov