FedVTE Training Catalog

SUMMER 2017

FedVTE FEDERAL VIRTUAL TRAINING ENVIRONMENT

Free cybersecurity training for government personnel.
fedvte.usalearning.gov

Welcome to the Federal Virtual Training Environment (FedVTE) Course Catalog!

Overview

The FedVTE Course Catalog provides an active listing of available cybersecurity training courses offered on the FedVTE training system. All courses have 24/7 accessibility, enabling users to take them at their own pace on their own schedule. All U.S. government employees and veterans are eligible for an account.

About the Workforce Framework

All FedVTE courses are aligned to the NICE Cybersecurity Workforce Framework, which is a national resource that describes cybersecurity work. It provides employers, employees, educators, students, and training providers with a common lexicon to speak about cybersecurity roles and jobs, and helps define professional requirements in cybersecurity. The Workforce Framework defines cybersecurity work into seven Categories. *(Refer to Figure 1 below.)*

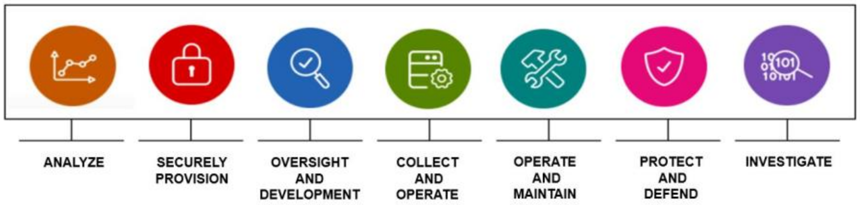
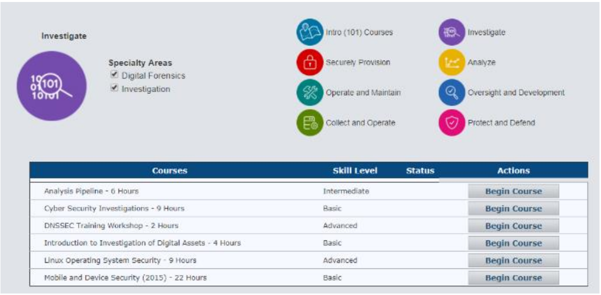


Figure 1 - NICE Cybersecurity Workforce Framework

Each of these Categories are comprised of several Specialty Areas that describe the involved cybersecurity tasks. It also provides a common set of knowledge, skills, and abilities (KSAs) necessary to perform within those Specialty Areas. By navigating and familiarizing with the Workforce Framework, current and aspiring cybersecurity professionals can quickly identify the courses needed to advance within his or her career, or transfer his or her skills to another cybersecurity track.

Navigating the Workforce Framework in FedVTE



Specialty Areas

☑ Digital Forensics

☑ Investigation

Courses	Skill Level	Status	Actions
Analysis Pipeline - 6 Hours	Intermediate		Begin Course
Cyber Security Investigations - 9 Hours	Basic		Begin Course
DNSSEC Training Workshop - 2 Hours	Advanced		Begin Course
Introduction to Investigation of Digital Assets - 4 Hours	Basic		Begin Course
Linux Operating System Security - 9 Hours	Advanced		Begin Course
Mobile and Device Security (2015) - 22 Hours	Basic		Begin Course

Figure 2 - Recommended Courses for Each Category

Users can navigate the provided Workforce Framework within FedVTE, to find courses that are aligned to specific Categories and Specialty Areas of interest. *(Refer to Figure 2.)*

Recently, an Intro (101) Courses Category has been added to help users easily locate beginner courses.

HOW TO SEARCH FOR COURSES:

After logging into your account:

1. Click on **My Courses**. *See Figure 1.*
2. Select on a **Workforce Framework Category**, based on your interests and training needs. *See Figure 2.*
    - Filter by **Specialty Areas**, as necessary.
    - Review list of courses aligned to the Category, Specialty Area, and skill level.

Note: *To see a full listing of courses, click* ***on All Courses*** *from the* ***My Courses*** *page.*

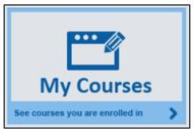
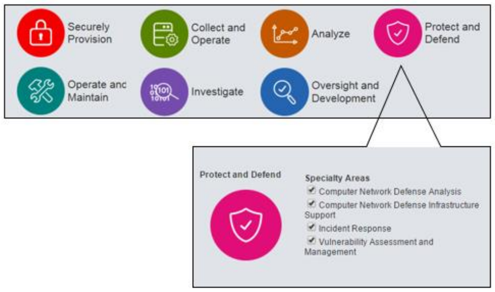


Figure 1. My Courses



Specialty Areas

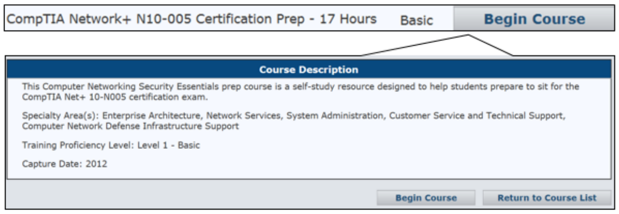
☑ Computer Network Defense Analysis
☑ Computer Network Defense Infrastructure Support
☑ Incident Response
☑ Vulnerability Assessment and Management

Figure 2. Workforce Framework Categories

HOW TO START COURSES:

3. Identify the course of interest.
4. Click on **Begin Course** to launch the course. *See Figure 3.*
    - A new window will appear.
5. Click on **Begin Course** to start the course.

Note: *Each course comprises of a series of modules that can be paused and resumed with its play bar. You can also download the corresponding Lesson PDF.*



CompTIA Network+ N10-005 Certification Prep - 17 Hours Basic

Course Description

This Computer Networking Security Essentials prep course is a self-study resource designed to help students prepare to sit for the CompTIA Net+ 10-N005 certification exam.

Specialty Area(s): Enterprise Architecture, Network Services, System Administration, Customer Service and Technical Support, Computer Network Defense Infrastructure Support

Training Proficiency Level: Level 1 - Basic

Capture Date: 2012

Figure 3. Launching and Starting the Course

Questions?

- For all technical-related questions, contact the FedVTE Online Training Portal Help Desk via email at Support@usalearning.net or by phone at 202-558-2203 from Monday to Friday between 8:30am and 6:00pm EST.
- For all non-technical questions, contact the FedVTE Program Office via email at FedVTE@hq.dhs.gov.

Training Courses

101 – Coding 5 Hours

In this course, you will learn the basics of computer programming - how to give a machine a set of instructions to produce a desired behavior. This course provides information on the elements of programming and programming languages, frameworks, and models. The course includes an interactive programming game, interactive knowledge checks, and the chance to write your own fully functional code.

Proficiency Level:	**Framework Category:**	**Specialty Areas:**
- Basic	- Securely Provision	- Software Assurance and Security Engineering - Systems Development - Systems Requirement Planning - Systems Security Architecture - Technology Research and Development - Test and Evaluation

101 – Critical Infrastructure Protection 2 Hours

In this course, you will learn about the influence, impact, and need for cybersecurity when defending the critical infrastructure and key resources of the United States. This course provides the definition of critical infrastructure, examples of cybersecurity threats to critical infrastructure, and information on what is being done to protect critical infrastructure from these cybersecurity threats.

Proficiency Level:	**Framework Category:**	**Specialty Areas:**
- Basic	- Securely Provision - Operate and Maintain - Oversight and Development - Protect and Defend	- Systems Architecture - Technology Research and Development - Systems Requirements Planning - Systems Development - Software Assurance and Security Engineering - Network Services - Systems Administration - Systems Analysis - Information Systems Security Operations - Security Program Management - Strategic Planning and Policy Development - Computer Network Defense Analysis - Computer Network Defense Infrastructure Support

101 – Reverse Engineering 2 Hours

In this course, you will learn the basics of reverse engineering, the process of analyzing a technology specifically to determine how it was designed or how it operates. Instead of working toward building a finished product (like you would in engineering), in reverse engineering you start with a finished product and try to work backwards to determine its component parts. This course focuses on reverse engineering computer software.

Proficiency Level:	**Framework Category:**	**Specialty Areas:**
- Basic	- Securely Provision	- Software Assurance and Security Engineering - Systems Development - Technology Research and Development

Advanced PCAP Analysis and Signature Dev (APA) 1 Hour

This course takes users through an introduction to rules, goes over example syntax, protocols and expressions. It contains several supporting video demonstrations as well as lab exercises writing and testing basic rules.

Proficiency Level:	**Framework Category:**	**Specialty Areas:**
- Intermediate	- Protect and Defend - Analyze	- Computer Network Defense Analysis - Exploitation Analysis - Incident Response

Advanced Windows Scripting 6 Hours

This course focuses on advanced concepts for writing scripts for the Microsoft Windows operating system. The course covers how to string multiple commands together in traditional BATCH scripts as well as leverage Visual Basic Scripting (VBS) to perform more complex tasks, and includes reinforcing video demonstrations and final assessment.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Operate and Maintain	- Network Services - System Administration - Systems Security Analysis

Analysis Pipeline 6 Hours

This course is designed for network flow data analysts who use or are considering using Analysis Pipeline. The course aims to help the student better understand how to incorporate streaming network flow analysis into their toolkit for identifying and alerting on events of interest. The focus will be on applying Analysis Pipeline to operational use cases.

Proficiency Level	Framework	Specialty Areas:
- Intermediate	- Protect and Defend	- Network Defense Analysis - Computer Network Defense - Infrastructure Support - Vulnerability Assessment and Management

CDM Module 1: Overview 2 Hours

This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding Continuous Diagnostics and Mitigation (CDM). The course aims to help the student better understand how CDM can help a department or agency (D/A) better manage risk and protect mission critical assets and to more effectively evaluate their cybersecurity posture.

The course provides a high level overview of the CDM program. Topics covered include basic CDM concepts, how CDM relates to NIST 800-53 and other NIST SPs, CDM Concept of Operations, the CDM Environment, and CDM's Phases and Capabilities.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Securely Provision - Oversight and Development	- Information Assurance Compliance - Information Systems Security Operations (Information Systems Security Officer) - Security Program Management (Chief Information Security Officer)

CDM Module 2: Hardware Asset Management 1 Hour

This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding Continuous Diagnostics and Mitigation (CDM). The course aims to help the student better understand how people and devices work together to protect mission critical assets and to more effectively evaluate their cybersecurity posture.

The course begins by defining Hardware Asset Management (HWAM) and why it is critical to the implementation of a robust cybersecurity program. The training highlights the criteria for monitoring and managing hardware assets using CDM. It then transitions into HWAM implementation criteria and discusses the generic CDM concept of operations specific to HWAM. Topics covered include Actual State, Desired State, and Defects.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Securely Provision - Oversight and Development	- Information Assurance Compliance - Information Systems Security Operations (Information Systems Security Officer)

		- Security Program Management (Chief Information Security Officer)

CDM Module 3: Software Asset Management 1.5 Hours

This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding CDM. The course aims to help the student better understand how people and software work together to protect mission critical assets and to more effectively evaluate their cybersecurity posture.

The course begins by defining Software Asset Management (SWAM) and why it is critical to the implementation of a robust cybersecurity program. It covers new roles and responsibilities which the D/A must implement. It then transitions into SWAM implementation criteria, and discusses the generic CDM concept of operations specific to SWAM Actual State, Desired State, and Defects. It includes high level discussions of software lists (white, gray, black) and how software can be identified and tracked in CDM through the use of Common Platform Enumeration (CPE) and Software Identification (SWID) tags by software package down to executables.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Securely Provision - Oversight and Development	- Information Assurance Compliance - Information Systems Security Operations (Information Systems Security Officer) - Security Program Management (Chief Information Security Officer)

CDM Module 4: Configuration Settings Management .5 Hour

This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding CDM. The course aims to help the student better understand CSM, provide organization visibility into risks associated with improper or non-compliant security-related configuration settings for authorized hardware and software.

The course begins by outlining the Cyber Security Manager position (CSM) and highlighting the types of attacks CSM can help prevent. It then transitions into CSM methods and criteria, where it reviews Actual State, Desired State, and Defect Checks specific to the capability area. It explains how CSM builds upon the other capabilities and how defect checks differ at the local and federal levels.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Securely Provision - Oversight and Development	- Information Assurance Compliance - Information Systems Security Operations (Information Systems Security Officer) - Security Program Management (Chief Information Security Officer)

CDM Module 5: Vulnerability Management .5 Hour

This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding CDM. The course aims to help the student better understand how vulnerability management (VULN) identifies the existence of vulnerable software products in the boundary to allow an organization to mitigate and thwart common attacks that exploit those vulnerabilities.

The course begins by defining VULN, how it applies to the target environment, and how a fully implemented VULN capability impacts a Department or Agency. It then transitions into VULN criteria and methods, where it reviews Actual State, Desired State, and Defect Checks specific to the capability area. It explains how VULN builds upon the other capabilities areas, the types of defects, and how those defect checks differ at the local and federal levels.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Securely Provision - Oversight and Development	- Information Assurance Compliance - Information Systems Security Operations (Information Systems Security Officer) - Security Program Management (Chief Information Security Officer)

Certified Ethical Hacker v9 (CEHv9) 31 Hours

The CEHv9 certification prep self-study course helps prepare students to sit for the EC-Council Certified Ethical Hacker version 9 certification exam. This course contains materials to aid the student in broadening their knowledge of advanced network assessment techniques including enumeration, scanning and reconnaissance. Updates to v9 from v8 include several new tools and new module on cloud considerations. Topics include reconnaissance, hacking laws, web application hacking, social engineering, packet capture, and scanning. The course then moves on to exploitation of several types of threats and how to cover your tracks, concluding with a practice exam.

Proficiency Level	**Framework**	**Specialty Areas:**
- Advanced	- Protect and Defend - Operate and Maintain	- Computer Network Defense Analysis - Systems Security Analysis - Vulnerability Assessment and Management

Certified Information Security Manager 2013 Self-Study Course 11 Hours

The Information Systems Audit and Control Association (ISACA) Certified Information Security Manager (CISM) certification prep course prepares students to sit for the management-focused CISM exam as well as strengthens their information security management expertise through the in-depth courseware and reinforcing demonstrations. Topics include information security governance, information risk management and compliance, information security program development and management, and information security incident management.

Proficiency Level	Framework	Specialty Areas:
- Intermediate	- Oversight and Development	- Systems Security Analysis - Computer Network Defense - Vulnerability Assessment and Management - Cyber Threat Analysis - Computer Network Defense Infrastructure Support

Cisco CCENT Self-Study Prep 13 Hours

The Cisco CCENT Prep course is a self-study resource for learners preparing for the Cisco CCENT certification, one of the prerequisites for the Cisco CCNA certification. Installing, operating, configuring, and verifying a basic IPv4 and IPv6 network will be discussed. Students will also be introduced to configuring a local area network (LAN) switch, configuring an internet protocol (IP) router, and identifying basic security threats. The course includes several reinforcing video demonstrations of concepts discussed, as well as a quiz.

Proficiency Level	Framework	Specialty Areas:
- Intermediate	- Operate and Maintain - Securely Provision	- Customer Service and Technical Support - Network Services - Systems Security Architecture

Cisco CCNA Security Self-Study Prep 15 Hours

The Cisco CCNA Security Self-Study Prep course is aimed at those who already have experience with routers and basic level networking skills, and those who may be interested in taking the Cisco CCNA Security exam. Content covered in the CCNA Security Prep course include protocol sniffers, analyzers, TCP/IP, desktop utilities, Cisco IOS, the Cisco VPN, a Cisco simulation program called Packet Tracer, and some web-based resources. Students will get a theoretical understanding of network security, knowledge and skills designed to implement it. This self-study resource contains several reinforcing video demonstrations and final exam.

Proficiency Level	Framework	Specialty Areas:
- Intermediate	- Operate and Maintain	- Customer Service and Technical Support - Network Services - System Administration

Cloud Computing Security 1 Hour

This course provides an in-depth look at the strengths and weaknesses of cloud computing security as well as the considerations to take in choosing the cloud as a data management solution. Technical and operational risks are explained, along with strategies to mitigate the aforementioned risks. To demonstrate concepts learned, the course closes with a real-world example of how a government agency (Defense Information Systems Agency) utilizes cloud computing solutions.

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Protect and Defend - Operate and Maintain	- Computer Network Defense Analysis - Systems Security Analysis - Vulnerability Assessment and Management

CMaaS Overview .5 Hour

This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding CDM. The course aims to help the student better understand how Continuous Monitoring as a Service (CMaaS) relates to the CDM program.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Oversight and Development - Protect and Defend	- Information Systems Security Operations - Security Program Management - Computer Network Defense Analysis - Computer Network Defense Infrastructure Support - Incident Response - Vulnerability Assessment and Management

CMaas Technical Overview .5 Hour

This course is designed for managers, staff and other stakeholders who may be involved in implementation and/or decision making regarding Continuous Diagnostics and Mitigation (CDM). The course aims to help the student better understand how Continuous Monitoring as a Service (CMaaS) will be implemented in DHS Component networks.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Protect and Defend	- Computer Network Defense Analysis - Computer Network Defense Infrastructure Support - Incident Response - Vulnerability Assessment and Management

CompTIA A+ (220 - 801) Certification Prep 12 Hours

The A+ 220-801 Certification Prep Self-Study is an introductory course presenting domain knowledge and objectives for the five domains featured in the A+ 220-801 portion of the A+ certification exam.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Operate and Maintain	- Customer Service and Technical Support - Network Services - System Administration

CompTIA A+ (220 - 802) Certification Prep 11 Hours

The A+ 220-802 Certification Prep Self-Study course is for entry-level IT professionals with at least 12 months experience in the field. Knowledge required for A+ candidates include installation, configuration, and maintenance of devices, PCs, and software for end users. This course contains materials for the four A+ 802 domains to aid the candidate in exam preparation.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Operate and Maintain	- Customer Service and Technical Support - Network Services - System Administration

CompTIA Advanced Security Practitioner (CASP) CAS-002 24 Hours

The CompTIA CASP certification prep course prepares students to sit for the CompTIA Advanced Security Practitioner CAS-002 certification exam by covering technical knowledge and skills required in designing and engineering secure solutions in enterprise environments. A broad spectrum of security disciplines are discussed to help with critical thinking when considering secure enterprise solutions and managing risk.

Proficiency Level	Framework	Specialty Areas:
- Advanced	- Operate and Maintain	- Network Services - System Administration - Systems Security Analysis

CompTIA Network+ (N10-005) Certification Prep 17 Hours

CompTIA's Network+ certification prep course was developed for the current Network+ exam code N10-005. Topics covered on the Network+ N10-005 exam as well as in this FedVTE prep course include network technologies, installation and configuration, media and topologies, management and security. This certification prep course includes video demonstrations, a practice exam, and hands-on labs.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Protect and Defend - Operate and Maintain	- Computer Network Defense Infrastructure Support - Customer Service and Technical Support - Network Services

CompTIA Security+ (SYO-401) Certification Prep 19 Hours

This certification prep course prepares students to sit for the CompTIA Security+ (SY0-401) certification exam as well as teaches concepts and techniques that are valuable to the workplace. Topics covered in the course, and competencies tested on the exam include network security, compliance and operational security, threats and vulnerabilities, application, data and host security, access control and identity management, and cryptography. This certification prep course includes several reinforcing video demonstrations as well as a practice quiz.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Protect and Defend - Operate and Maintain	- Computer Network Defense Analysis - Systems Security Analysis - Vulnerability Assessment and Management

Cyber Investigations 8 Hours

This course serves as an introduction and overview of several concepts and technologies that may be encountered as part of an investigation with a digital or cyber component. Starting with the basics of how devices communicate, the course continues with technical concepts and applications that may be used to facilitate or investigate incidents. Content includes lab exercises and practical application takeaways to reinforce concepts, and a course exam.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Analyze - Investigate	- Threat Analysis - Digital Forensics

Cyber Risk Management for Managers 6 Hours

Cyber Risk Management for Managers covers key concepts, issues, and considerations for managing risk from a manager’s perspective. Discussions include identifying critical assets and operations, a primer on cyber threats and how to determine threats to your business function, mitigation strategies, and response and recovery.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Oversight and Development	- Information Systems Security Operations (Information Systems Security Officer) - Legal Advice and Advocacy - Strategic Planning and Policy Development

Cyber Risk Management for Technicians 11 Hours

This course presents the concept of managing cyber risk from a technical perspective. An overview of cyber risk management opens the class, followed by foundational material on conducting a risk assessment of considerations such as threats, vulnerabilities, impacts, and likelihood. Various technical methods for conducting a risk assessment are presented, to include vulnerability assessments and penetration tests, with a focus on continuous monitoring of security controls and how to assess those security controls using the National Institute of Standards and Technology Special Publication 800-53 and 800-53a as a guide.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Oversight and Development	- Information Systems Security Operations (Information Systems Security Officer) - Security Program Management (Chief Information Security Officer) - Strategic Planning and Policy Development

Cyber Security Investigations 9 Hours

This course discusses the basic concepts of cyber security and digital forensics investigation practices. Topics include performing collection and triage of digital evidence in response to an incident, evidence collection methodologies, and forensic best practices. This is an introductory course reviewing the processes, methods, techniques and tools in support of cybersecurity investigations.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Collect and Operate - Investigate - Protect and Defend	- Cyber Operations - Digital Forensics - Incident Response

Cyber Security Overview for Managers 6 Hours

Cybersecurity Overview for Managers is designed for managers and other stakeholders who may be involved in decision making regarding their cyber environment but do not have a strong technical background. Discussions will not focus on specific technologies or implementation techniques, but rather cybersecurity methodologies and the framework for providing a resilient cyber presence. The course aims to help managers better understand how people and devices work together to protect mission critical assets and more effectively evaluate their cyber posture.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Oversight and Development	- Information Systems Security Operations (Information Systems Security Officer) - Security Program Management (Chief Information Security Officer) - Strategic Planning and Policy Development

DB Evaluations using AppDetectivePro and dbProtect 1.5 Hours

This course introduces students to basic database security concepts and methodology. The course demonstrates how tools such as AppDetectivePRO and DbProtect can be used to scan databases in order to uncover configuration mistakes, identification and access control issues, missing patches, or any toxic combination of settings which could lead to escalation-of-privilege or denial-of-service attacks, data leakage, or unauthorized modification of data.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Securely Provision	- Information Assurance Compliance - Software Assurance and Security Engineering - Systems Development - Test and Evaluation

Demilitarized Zone (DMZ) with IDS/IPS 9 Hours

This course introduces the concept of a network Demilitarized Zone (DMZ) and the security benefits it can provide. Best practices for designing and implementing a DMZ is followed with a section on IDS and IPS systems that includes an in-depth look at SNORT for network monitoring. The course concludes with log analysis and management best practices.

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Protect and Defend - Operate and Maintain	- Computer Network Defense Infrastructure Support - Network Services - Systems Security Analysis

DNSSEC Training Workshop 2 Hours

This course covers the basics of DNSSEC, how it integrates into the existing global DNS and provides a step-by-step process to deploying DNSSEC on existing DNS zones.

Proficiency Level	Framework	Specialty Areas:
- Advanced	- Securely Provision - Oversight and Development	- Systems Security Architecture - Network Services - System Administrator

DoD IA Boot Camp 12 Hours

The Department of Defense Insurance Assurance (DoD IA) Boot Camp is an in-depth study program designed so students may successfully perform their duties as IA professionals, to include Information Assurance Managers, Information Assurance Officers, or System Administrators with IA duties. This course will provide the student with DoD policy guidance as related to law, policy, technical implementation guidance, documentation requirements, and references necessary to support a successful DoD IA program.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Securely Provision - Oversight and Development	- Information Assurance Compliance - Strategic Planning and Policy Development

Dynamic Testing using HPE WebInspect 1.5 Hours

This course introduces students to dynamic testing tools for web applications and demonstrates how they can be used to identify, evaluate, and mitigate a web application's potential security vulnerabilities. The focus is on using HPE WebInspect; in order to perform and manage dynamic security vulnerability testing and address results from both a developer and cybersecurity professional perspective.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Securely Provision	- Information Assurance Compliance - Software Assurance and Security Engineering - Systems Development - Test and Evaluation

Emerging Cyber Security Threats 12 Hours

This course covers a broad range of cyber security elements that pose threats to information security posture. The various threats are covered in detail, followed by mitigation strategies and best practices.

This course will cover what policy is, the role it plays in cybersecurity, how it is implemented, and cybersecurity laws, standards, and initiatives. Topics include cybersecurity policy, knowing your enemy, mobile device security, cloud computing security, Radio Frequency Identification (RFID) security, LAN security using switch features, securing the network perimeter, securing infrastructure devices, security and DNS and IPv6 security. Video demonstrations are included to reinforce concepts.

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Oversight and Development - Operate and Maintain - Protect and Defend	- Strategic Planning and Policy Development - System Administration - Vulnerability Assessment and Management

Foundations of Incident Management 10.5 Hours

This course provides an introduction to the basic concepts and functions of incident management. The course addresses where incident management activities fit in the information assurance or information security ecosystem and covers the key steps in the incident handling lifecycle with practices to enable a resilient incident management capability.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Protect and Defend	- Computer Network Defense Infrastructure Support - Incident Response

Introduction to Investigation of Digital Assets 4 Hours

This course is designed for technical staff who are new to the area of Digital Media Analysis and Investigations. It provides an overview of the digital investigation process and key activities performed throughout the process and various tools that can be used to perform each activity.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Collect and Operate - Investigate	- Collection Operations - Digital Forensics - Investigation

Introduction to Threat Hunting Teams 1.5 Hours

This course provides basic definitions, activities, and examples of teams hunting threats in the cyber domain. The course addresses the differences between hunting team activities and those of incident management teams or penetration testing teams. The content covers how hunting teams establish goals, methods used by threat hunting teams, and sources available to help read and interpret the threat landscape.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Protect and Defend - Analyze	- Computer Network Defense Analysis - Threat Analysis

Introduction to Windows Scripting 4 Hours

This course focuses on writing scripts for the Microsoft Windows operating system. It covers fundamentals and syntax for automating administrative and security monitoring tasks. The course will present the basics of Windows BATCH scripting syntax and structure, along with several Windows command line utilities to harness the powerful capabilities built into Windows.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Operate and Maintain	- Network Services - System Administration - Systems Security Analysis

IPv6 Security Essentials 5 Hours

This Internet Protocol version 6 (IPv6) Security Essentials course begins with a primer of IPv6 addressing and its current deployment state, discusses Internet Control Manager Protocol version 6 (ICMPv6), Dynamic Host Configuration Protocol version 6 (DHCPv6), and Domain Name System version 6 (DNSv6), and concludes with IPv6 Transition Mechanisms, security concerns and management strategies. This course includes several reinforcing video demonstrations, as well as a final knowledge assessment.

Proficiency Level	Framework	Specialty Areas:
- Advanced	- Protect and Defend - Operate and Maintain	- Computer Network Defense Analysis - Network Services - System Administration

(ISC)2™ CAP (R) Certification Prep 11 Hours

This certification prep course is designed to help prepare students for the Information Security Certification (ISC)2 Certified Authorization Professional (CAP) certification exam as well as strengthen their knowledge and skills in the process of authorizing and maintaining information systems. Topics include understanding the Risk Management Framework (RMF), selection, implementation, and monitoring of security controls as well as the categorization of information systems. The course includes a practice exam.

Proficiency Level	Framework	Specialty Areas:
- Intermediate	- Protect and Defend - Operate and Maintain	- Computer Network Defense Analysis - Systems Security Analysis - Vulnerability Assessment and Management

(ISC)2™ CSSLP: Certification Prep 20 Hours

This certification prep course helps prepare students to sit for the (ISC)2 CSSLP certification exam by covering application security concepts and the software development lifecycle (SDLC). This course is for individuals with at least four years of experience in secure software concepts, software requirements, software design, and software implementation.

Proficiency Level	Framework	Specialty Areas:
- Advanced	- Securely Provision - Oversight and Development - Operate and Maintain	- Software Assurance and Security Engineering - Strategic Planning and Policy Development - Systems Security Analysis

(ISC)2™ CISSP®: ISSEP Certification Prep 12 Hours

The Information Systems Security Engineering Professional (ISSEP) concentration of the Certified Information Systems Security Professional (CISSP) certification prep course prepares students with systems security engineering experience to sit for the (ISC)2 ISSEP certification exam. This course includes a 100-question practice exam and was developed following the four domains of the ISSEP.

Proficiency Level	Framework	Specialty Areas:
- Advanced	- Oversight and Defend - Operate and Maintain - Securely Provision	- Strategic Planning and Policy Development - System Administration - Systems Requirements Planning

(ISC)2™ CISSP®: ISSAP Certification Prep 15 Hours

The Information Systems Security Architecture Professional (ISSAP) concentration of the CISSP certification prep course prepares students with security architect and analyst experience to sit for the (ISC)2 ISSAP certification exam. This course includes a practice exam and reinforcing video demonstrations for many of the topics included in the six domains of the ISSAP.

Proficiency Level	Framework	Specialty Areas:
- Advanced	- Operate and Maintain - Securely Provision	- System Administration - Systems Requirements Planning - Systems Security Architecture

(ISC)2™ CISSP®: ISSMP Certification Prep (2014) 14 Hours

The Information Systems Security Management Professional (ISSMP) concentration of the CISSP certification prep course prepares students with management experience to sit for the (ISC)2 ISSMP certification exam. This course includes a 100-question practice exam and includes video demonstrations reinforcing many of the topics included in the five domains of the ISSMP.

Proficiency Level	Framework	Specialty Areas:
- Advanced	- Oversight and Development	- Information Systems Security Operations (Information Systems Security Officer) - Security Program Management (Chief Information Security Officer) - Strategic Planning and Policy Development

(ISC)2™ CISSP ® Prep 2015 25 Hours

The (ISC)2 Certified Information Systems Security Professional (CISSP) certification self-study prep course is a resource for individuals preparing for the CISSP certification exam or expanding their knowledge in the information security field. The course reflects the 2015 published CISSP exam objectives and the eight domains upon which the exam is based. This course also includes domain quizzes, reinforcing video demonstrations, as well as a final practice exam.

Proficiency Level	Framework	Specialty Areas:
- Advanced	- Securely Provision - Oversight and Development	- Information Assurance Compliance - Information Systems Security Operations (Information Systems Security Officer) - Security Program Management (Chief Information Security Officer)

(ISC)2™ Systems Security Certified Practitioner 16 Hours

The Systems Security Certified Practitioner (SSCP) certification prep course is a self-study resource for those preparing to take the (ISC)2 SSCP certification exam as well as those looking to increase their understanding of information security concepts and techniques. The certification is described as being ideal for those working toward positions such as network security engineers, security systems analysts, or security administrators. This course, complete with a 100-question practice exam and video demonstrations, was developed based on the seven SSCP domains prior to the April 15, 2015 (ISC)2 ™ domain update. A new, updated course is currently in development.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Protect and Defend - Operate and Maintain	- Computer Network Defense Analysis - Network Services - Systems Security Analysis

ISACA Certified Information Systems Auditor(CISA) 20 Hours

The Information Systems Auditing prep course is a self-study resource designed to help students prepare to sit for the ISACA Certified Information Systems Auditor (CISA) exam.

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Protect and Defend - Operate and Maintain	- Computer Network Defense Analysis - Systems Security Analysis - Vulnerability Assessment and Management

LAN Security Using Switch Features 2 Hours

In this course, students learn different methods of how to secure Local Area Networks (LANs) at the connectivity level. Topics include: monitoring media access control (MAC) addresses and port security, limiting MAC & IP spoofing, controlling traffic flows, implementing and enhancing security in virtual local area network (VLANs), enabling authentication on connection points, and determining host security health. Examples are used throughout to reinforce concepts.

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Operate and Maintain - Protect and Defend	- System Administration - Systems Security Analysis - Vulnerability Assessment and Management

Linux Operating System Security 9 Hours

This course introduces students to the security features and tools available in Linux as well as the considerations, advantages, and disadvantages of using those features. The class will be based on Red Hat Linux and is designed for IT and security managers, and system administrators who want to increase their knowledge on configuring and hardening Linux from a security perspective.

Proficiency Level	**Framework**	**Specialty Areas:**
- Advanced	- Investigate - Protect and Defend - Operate and Maintain	- Digital Forensics - Incident Response - Systems Security Analysis

Mobile Forensics 4 Hours

This course provides an overview of mobile forensics, the branch of digital forensics that focusses on forensically sound extraction and analysis of evidence from mobile devices. Cell phone investigations has grown exponentially with data from mobile devices becoming crucial evidence in a wide array of incidents. The Mobile Forensics course begins highlighting details of the field and then focuses on the iOS architecture, concluding with data acquisition and analysis.

Proficiency Level	**Framework**	**Specialty Areas:**
- Advanced	- Investigate	- Digital Forensics - Investigation

Mobile and Device Security 22 Hours

Updated in 2015, the Mobile and Device Security course introduces students to mobile devices, how they operate, and their security implications. This course includes topics such as signaling types, application stores, managing mobile devices, and emerging trends and security and privacy concerns with social media.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Operate and Maintain - Investigate - Securely Provision	- Customer Service and Technical Support - Digital Forensics - Information Assurance Compliance

Network Layer 1 & 2 Troubleshooting 3 Hours

This course reviews troubleshooting methods used in Layer 1 and Layer 2 of the OSI Model. The course covers how to detect, trace, identify, and fix network connectivity issues at the Physical and Data Link layers of the OSI stack. The basics of the Physical and Data Link layers will be covered along with a review of the devices, signaling, and cabling which operate at these layers. Students will be presented with methods for tracing connectivity issues back to the source and identifying mitigation solutions.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Operate and Maintain	- Customer Service and Technical Support - Network Services - System Administration

Network Monitoring with Open Source Tools 5 Hours

The Network Monitoring with Open Source Tools course was designed to give the learner a general awareness of network security and monitoring concepts. Discussions and demonstrations focus on network threats, and the capabilities of tools. After completion of the course, students should be able to detect attacks using network monitoring tools.

Proficiency Level	**Framework**	**Specialty Areas:**
- Advanced	- Protect and Defend - Operate and Maintain	- Computer Network Defense Analysis - Incident Response - Systems Security Analysis

Offensive and Defensive Network Operations 13 Hours

This course focuses on fundamental concepts for offensive and defensive network operations. It covers how offensive and defensive cyber operations are conducted and details U.S. government doctrine for network operations. Topics include network attack planning, methodologies, and tactics and techniques used to plan for, detect, and defend against network attacks.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Protect and Defend - Collect and Operate	- Computer Network Defense Analysis - Cyber Operations

Penetration Testing 14 Hours

The Penetration Testing course discusses concepts, tools, and techniques for conducting a penetration test. The course lays the groundwork with familiar ethical hacking concepts, moves into penetration testing methods, and determines the most effective penetration tool for the desired goal.

Proficiency Level	**Framework**	**Specialty Areas:**
- Advanced	- Protect and Defend - Operate and Maintain	- Computer Network Defense Analysis - Systems Security Analysis - Vulnerability Assessment and Management

Radio Frequency Identification (RFID) Security 1 Hour

This course will cover securing radio frequency identification (RFID). Different components of RFID, how it works, applications in which it is being used, benefits and weaknesses, and the communication range over which it works will be reviewed. Students will learn specific concerns with RFID, recommendations for RFID, and security issues that have come to light.

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Operate and Maintain - Protect and Defend	- Systems Security Analysis - Vulnerability Assessment and Management

Root Cause Analysis 1 Hour

This course provides an explanation of root cause analysis for cybersecurity incidents and an overview of two different root cause analysis models (and approaches used in these models). The course also describes how root cause analysis can benefit other incident management processes (response, prevention, and detection), and details general root cause analysis techniques that can be adopted as methods for analysis of cyber incidents.

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Securely Provision	- Software Assurance and Security Engineering

Securing Infrastructure Devices 1 Hour

This course covers physical security, operating system security, management traffic security, device service hardening, securing management services and device access privileges.

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Protect and Defend - Operate and Maintain - Securely Provision	- Computer Network Defense Infrastructure Support - Network Services - Systems Security Architecture

Securing the Network Perimeter 1 Hour

This course covers edge security traffic design, blocking denial of service/ distributed denial of service (DoS/DDoS) traffic, specialized access control lists, routers and firewalls, securing routing protocols, securing traffic prioritization and securing against single point of failure (SPOF).

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Protect and Defend - Operate and Maintain	- Computer Network Defense Analysis - Incident Response - Network Services

Security and DNS 1 Hour

This course discusses name resolution principles, name resolution and security, DNS security standards, securing zone transfers with transaction signature (TSIG), and DNS Security Extension (DNSSEC) principles, implementation and resources.

Proficiency Level	**Framework**	**Specialty Areas:**
- Advanced	- Operate and Maintain	- Network Services - System Administration

SILK Traffic Analysis 7 Hours

This course is designed for analysts involved in daily response to potential cyber security incidents, and who have access to the Einstein environment. The course begins with an overview of network flow and how the SiLK tools collect and store data. The next session focuses specifically on the Einstein environment. The basic SiLK tools are covered next, giving the analyst the ability to create simple analyses of network flow. Advanced SiLK tools follow, and cover how to create efficient and complex queries. The course culminates with a lab where students use their new skills to profile a network.

Proficiency Level	Framework	Specialty Areas:
- Intermediate	- Protect and Defend - Analyze	- Computer Network Defense Analysis - Exploitation Analysis - Vulnerability Assessment and Management

Software Assurance Executive Course (SAE) 10 Hours

This course is designed for executives and managers who wish to learn more about software assurance as it relates to acquisition and development. The purpose of this course is to expose participants to concepts and resources available now for their use to address software security assurance across the acquisition and development life cycles.

Proficiency Level	Framework	Specialty Areas:
- Intermediate	- Securely Provision	- Software Assurance and Security Engineering - Systems Requirements Planning - Technology Research and Development

Static Code Analysis using HPE Fortify 2 Hours

This course introduces students to the idea of integrating static code analysis tools into the software development process from both a developer's and a security professional's perspective. The course demonstrates how HPE Fortify is used to identify and remove Common Weakness Enumeration (CWE) from applications in which the source code is available.

Proficiency Level	Framework	Specialty Areas:
- Basic	- Securely Provision	- Information Assurance Compliance - Software Assurance and Security Engineering - Systems Development

Static Code Analysis using Synopsis Coverity 1.5 Hours

This course introduces students to the idea of integrating static code analysis tools into the software development process. The focus is on how developers can use tools such as Coverity to identify and remove Common Weakness Enumeration (CWE) from applications in which the source code is available, prior to deployment.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Securely Provision	- Information Assurance Compliance - Software Assurance and Security Engineering - Systems Development - Test and Evaluation

Supply Chain Assurance using Sonatype Nexus 2.5 Hours

This course introduces students to the idea of integrating static code analysis tools into the software development process from both, a developer's and a security professional's perspective. The course demonstrates how tools such as Sonatype Nexus can be used to evaluate the software supply chain in order to identify and remove components with known Common Vulnerabilities and Exposures (CVE) from applications in which the source code is available.

Proficiency Level	**Framework**	**Specialty Areas:**
- Basic	- Securely Provision	- Information Assurance Compliance - Software Assurance and Security Engineering - Systems Development - Systems Requirements Planning - Systems Security Architecture - Technology Research and Development - Test and Evaluation

Windows Operating System Security 16 Hours

This course introduces students to the security aspects of Microsoft Windows. The class begins with an overview of the Microsoft Windows security model and some key components such as processes, drivers, the Windows registry, and Windows kernel. An overview of the users and group permission structure used in Windows is presented along with a survey of the attacks commonly seen in Windows environments. Patching, networking, and the built-in security features of Windows such as the firewall, anti-malware, and BitLocker are all covered in light detail.

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Operate and Maintain - Protect and Defend	- System Administration - Systems Security Analysis - Vulnerability Assessment and Management

Wireless Network Security (WNS) 9 Hours

The purpose of the Wi-Fi Communications and Security course is to teach the technologies of the 802.11 family of wireless networking, including the principles of network connectivity and network security. The course is designed to provide a relevant, high-level overview of many elements that are critical components in Wi-Fi networking and security.

Proficiency Level	**Framework**	**Specialty Areas:**
- Intermediate	- Operate and Maintain	- Customer Service and Technical Support - Network Services - System Administration