Welcome to the Cybersecurity & Infrastructure Security Agency Cybersecurity Workforce Training Guide!

The Cybersecurity and Infrastructure Security Agency (CISA) developed this Guide to help prospective and current cyber professionals understand how to chart a prosperous career path. As a cybersecurity professional, you are at the forefront of CISA's mission to mitigate risks to our Nation's critical infrastructure. You play a crucial role in securing cyber space and critical infrastructure – from information technology and government facilities to emergency services and healthcare — that form the backbone of our communities. To put this mission into practice, you must keep your skills sharp, so you're ready to tackle any new challenge.

This Cybersecurity Workforce Training Guide is a tool to help you:

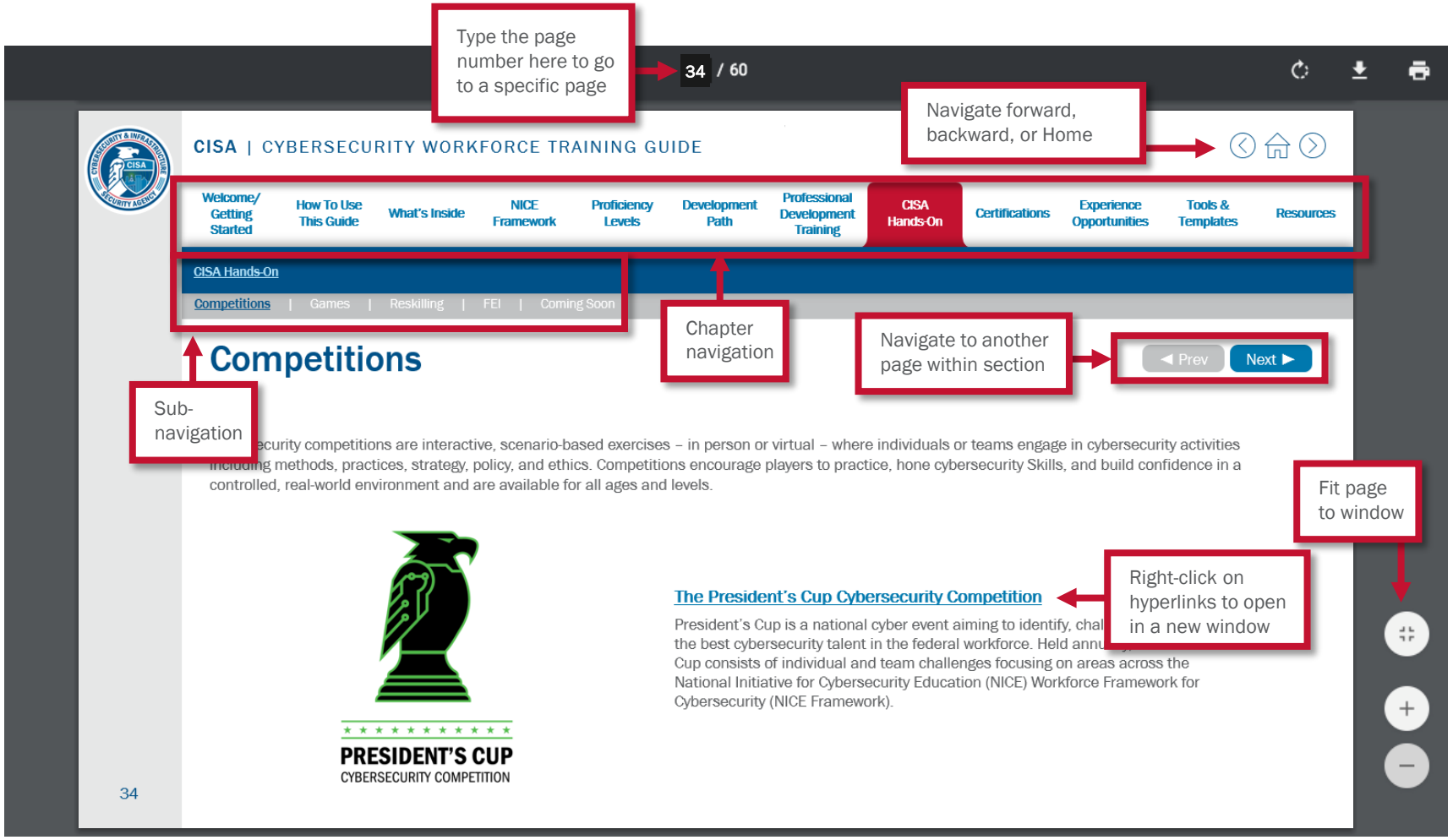
- Identify your job track so you can pinpoint areas for growth
- Understand the Work Roles, Tasks, and Knowledge, Skills, and Abilities (KSAs) that are your keys to success
- Discover training and professional development opportunities to build your skills and maximize your potential

CISA is committed to helping you grow your career by providing access to training and tools for advancement. This Guide is the first step to help you chart your path to future success in the federal and state, local, tribal, and territorial (SLTT) cybersecurity communities. It's up to you to take the next step and make the most of it. So, are you ready to get started? Continue reading to learn how to use this Guide.

How to Use this Guide

Interactive Elements

Use the navigation menus and tabs to jump to any page in this Guide.



How to Use this Guide

User Roles

You can use this Guide in different ways based on your role in cybersecurity.

If you are a current or future federal and SLTT cybersecurity staff member

Develop a roadmap for your career development – this Guide is a tool you can use to take a self-guided tour of development activities that will help you advance. You can also use this Guide to open a dialogue with your manager about your strengths, areas for improvement, and career goals.

If you are a Cybersecurity Manager

Identify skill gaps in your workforce – you can then work with your staff to identify training courses to resolve the gaps. This Guide should help to engage and empower your workforce to achieve your organization's cybersecurity objectives.

If you are in Human Resources

You can use this Guide to better understand what Knowledge, Skills, and Abilities are needed for different positions within your organization and factor them into the recruiting and hiring process.

What's Inside

This Guide is broken down into five sections. Each section builds upon the previous one, so you should review the Guide in order your first time through. Then, use the 12 tabs in the above Navigation Menu to jump around and find the information you need.

Part 1

Welcome/Getting Started, How to Use This Guide, & What's Inside

These sections explain the purpose of this Guide and show you how to use the features.

Part 2

NICE Framework and Proficiency Levels

These sections begin to set the foundation and understanding of the NICE Framework and personalize your career path by defining the various Categories, Specialty Areas, and Work Roles in cybersecurity and the proficiency level that applies to you.

Part 3

Development Path

This section outlines the steps to map out your career development path. It shows you how to apply the concepts from Parts 1-2 to customize a plan just for you.

Part 4

Professional Development Training, CISA Hands-On, Certifications, and Experience Opportunities

These sections let you explore a multitude of training and development activities to feed right into a personalized Cybersecurity Training Plan and drive your career journey.

Part 5

Tools & Templates, and Resources

This section provides a worksheet and sample development path to help you get started.

NICE Framework

What is the NICE Framework?

The National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181r1, is a nationally focused resource that categorizes and describes cybersecurity work. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors.

	Definition
Categories / Specialty Areas	A high-level grouping of common cybersecurity functions. Categories contain groupings of cybersecurity work, which are called Specialty Areas. Each Specialty Area represents an area of concentrated work, or function, within cybersecurity and related work.
Work Roles	The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of Knowledge, Skills, and Abilities (KSAs) and a list of Tasks performed in that role.
Tasks	Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles.
Knowledge	The factual or procedural information that you need to perform a Task. Knowledge is gained through training, research, and hands-on experience.
Skills	The result of applying your knowledge to perform a Task. Skills are developed and refined with practice and training.
Abilities	The potential or capability to perform Tasks.

Why is the NICE Framework Important?

The NICE Framework enables the use of a consistent, comparable, and repeatable approach to select and specify cybersecurity roles for positions within organizations. It also provides a common lexicon that academic institutions can use to develop cybersecurity curricula that better prepares students for current and future cybersecurity workforce needs.

NICE Framework

Categories

Categories are high-level groupings of common cybersecurity functions. There are seven Categories, each comprised of Specialty Areas and Work Roles with corresponding KSAs. Learn more about the Categories, Specialty Areas, and Work Roles next.

1. Analyze
2. Collect and Operate
3. Investigate
4. Operate and Maintain
5. Oversee and Govern
6. Protect and Defend
7. Securely Provision

Why are Categories Important?

Categories provide the overarching organizational structure of the NICE Framework. This structure is based on extensive job analyses, which group together work and workers that share major common functions, regardless of job titles or other occupational terms.

NICE Framework

Specialty Areas

◄ Prev Next ►

Specialty Areas represent an area of concentrated work, or function, within cybersecurity and related work. Each Specialty Area includes numerous Work Roles with the specific attributes needed to perform them in the form of Tasks and KSAs. Scroll through the Specialty Areas to learn more.

Analyze

Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

- All Source Analysis
- Exploitation Analysis
- Language Analysis
- Targets
- Threat Analysis

Collect and Operate

Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

- Collection Operations
- Cyber Operational Planning
- Cyber Operations

Why are Specialty Areas Important?

Specialty Areas define specific areas of specialty within the cybersecurity domain. A Specialty Area belongs to one and only one cybersecurity category but can have any number of unique Tasks and KSAs associated with it.

For a deeper dive into the Specialty Areas, visit CISA's NICCS website Workforce Development Section.

NICE Framework

Specialty Areas

◄ Prev Next ►

Specialty Areas represent an area of concentrated work, or function, within cybersecurity and related work. Each Specialty Area includes numerous Work Roles with the specific attributes needed to perform them in the form of Tasks and KSAs. Scroll through the Specialty Areas to learn more.

Investigate

Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

- Cyber Investigation
- Digital Forensics

Operate and Maintain

Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

- Customer Support and Technical Support
- Data Administration
- Knowledge Management
- Network Services
- Systems Administration
- Systems Analysis

Why are Specialty Areas Important?

Specialty Areas define specific areas of specialty within the cybersecurity domain. A Specialty Area belongs to one and only one cybersecurity category but can have any number of unique Tasks and KSAs associated with it.

For a deeper dive into the Specialty Areas, visit CISA's NICCS website Workforce Development Section.

NICE Framework

Specialty Areas

◄ Prev Next ►

Specialty Areas represent an area of concentrated work, or function, within cybersecurity and related work. Each Specialty Area includes numerous Work Roles with the specific attributes needed to perform them in the form of Tasks and KSAs. Scroll through the Specialty Areas to learn more.

Oversee and Govern

Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

- Cybersecurity Management
- Executive Cyber Leadership
- Legal Advice and Advocacy
- Program/Project Management and Acquisition
- Strategic Planning and Policy
- Training, Education, and Awareness

Protect and Defend

Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

- Cyber Defense Analysis
- Cyber Defense Infrastructure Support
- Incident Response
- Vulnerability Assessment and Management

Why are Specialty Areas Important?

Specialty Areas define specific areas of specialty within the cybersecurity domain. A Specialty Area belongs to one and only one cybersecurity category but can have any number of unique Tasks and KSAs associated with it.

For a deeper dive into the Specialty Areas, visit CISA's NICCS website Workforce Development Section.

NICE Framework

Specialty Areas

◄ Prev Next ►

Specialty Areas represent an area of concentrated work, or function, within cybersecurity and related work. Each Specialty Area includes numerous Work Roles with the specific attributes needed to perform them in the form of Tasks and KSAs. Scroll through the Specialty Areas to learn more.

Securely Provision

Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or networks development.

- Risk Management
- Software Development
- System Architecture
- Systems Development
- Systems Requirements Planning
- Technology R&D
- Test and Evaluation

Why are Specialty Areas Important?

Specialty Areas define specific areas of specialty within the cybersecurity domain. A Specialty Area belongs to one and only one cybersecurity category but can have any number of unique Tasks and KSAs associated with it.

For a deeper dive into the Specialty Areas, visit CISA's NICCS website Workforce Development Section.

NICE Framework

Work Roles

◄ Prev Next ►

Work Roles are a way to describe a grouping of work for which someone is responsible or accountable. Work Role names are not synonymous with job titles or occupations.

Work Roles 1-18

- All Source - Collection Manager
- All Source - Collection Requirements Manager
- All Source - Analyst
- Authorizing Official/Designating Representative
- Communications Security (COMSEC) Manager
- Cyber Crime Investigator
- Cyber Defense Analyst
- Cyber Defense Forensics Analyst
- Cyber Defense Incident Responder
- Cyber Defense Infrastructure Support Specialist
- Cyber Instructional Curriculum Developer
- Cyber Instructor
- Cyber Intel Planner
- Cyber Legal Advisor
- Cyber Operator
- Cyber Ops Planner
- Cyber Policy and Strategy Planner
- Cyber Workforce Development Manager

Why are Work Roles Important?

Work Roles are composed of Tasks that constitute work to be done; Tasks include associated Knowledge and Skill statements that represent learners' potential to perform those Tasks.

For a comprehensive look at the various Tasks and KSAs related to each Work Role on CISA's NICCS NICE Framework Work Roles Page.

NICE Framework

◄ Prev Next ►

Work Roles

Work Roles are a way to describe a grouping of work for which someone is responsible or accountable. Work Role names are not synonymous with job titles or occupations.

Work Roles 19 - 36

- Data Analyst
- Data Administrator
- Enterprise Architect
- Executive Cyber Leadership
- Exploitation Analyst
- Information Systems Security Developer
- Information Systems Security Manager
- IT Investment/Portfolio Manager
- IT Program Auditor
- IT Project Manager
- Knowledge Manager
- Law Enforcement/Counterintelligence Forensics Analyst
- Mission Assessment Specialist
- Multi-disciplined Language Analyst
- Network Operations Specialist
- Partner Integration Planner
- Privacy Officer/Privacy Compliance Manager
- Product Support Manager

Why are Work Roles Important?

Work Roles are composed of Tasks that constitute work to be done; Tasks include associated Knowledge and Skill statements that represent learners' potential to perform those Tasks.

For a comprehensive look at the various Tasks and KSAs related to each Work Role on CISA's NICCS NICE Framework Work Roles Page.

NICE Framework

◄ Prev Next ►

Work Roles

Work Roles are a way to describe a grouping of work for which someone is responsible or accountable. Work Role names are not synonymous with job titles or occupations.

Work Roles 37 - 52

- Program Manager
- Research and Development Specialist
- Secure Software Assessor
- Security Architect
- Security Control Assessor
- Software Developer
- System Administrator
- System Testing and Evaluation Specialist
- System Requirements Planner
- System Security Analyst
- Target Developer
- Target Network Analyst
- Technical Support Specialist
- Threat/Warning Analyst
- Vulnerability Assessment Analyst

Why are Work Roles Important?

Work Roles are composed of Tasks that constitute work to be done; Tasks include associated Knowledge and Skill statements that represent learners' potential to perform those Tasks.

For a comprehensive look at the various Tasks and KSAs related to each Work Role on CISA's NICCS NICE Framework Work Roles Page.

National Initiative for Cybersecurity Careers and Studies

◄ Prev Next ►

NICCS Website

The National Initiative for Cybersecurity Careers and Studies (NICCS) website is the premier online resource for cybersecurity training courses. NICCS easily connects everyone with cybersecurity training providers throughout the Nation, from government employees and senior cyber professionals to students, educators, and industry.

Highlights

- Over 6,000 cybersecurity-related training courses to choose from in the NICCS Education & Training Catalog – both virtual and in-person, no cost and paid. Find courses to help you improve your skill set, increase your level of expertise, earn a certification, or even transition into a new career.
- NICE Framework Mapping Tool – take the guesswork out of using the NICE Framework! Enter information about a cyber position and generate a report to better understand how well you align to the NICE Framework.
- **NEW!** Cyber Career Pathways Tool – an interactive way to explore the key attributes of the NICE Framework Work Roles and plan out your cybersecurity career path.
- Cybersecurity curricula and resources for teachers and students in grades Kindergarten through 12th grade (K-12) such as course content, posters, brochures, tip cards, and more.
- Veterans User Guide and Communications Manual has resources for individuals looking to transition from military service into a career in cybersecurity including scholarship information for those looking to go back to school.

Note on NICCS Training

Even though CISA provides free training for federal and SLTT employees, there could be a need to seek paid training. CISA's NICCS Education and Training Catalog lists training providers nation-wide.

Check with your supervisor first; requests must be approved by your supervisor before registering for external trainings that cost money.

What are Proficiency Levels?

Proficiency is used to indicate a degree of capability or expertise in a specific Knowledge, Skill, or Ability that allows one to function independently in performing that Knowledge or Skill. Proficiencies also provide a mechanism for organizations to assess learners. Work Roles are composed of Tasks that constitute work to be done; Tasks include associated Knowledge and Skill statements that represent learners' potential to perform those Tasks. Proficiency is not aligned to position level or to pay scale such as the General Schedule (GS) for government employees.

There are three proficiency levels. Click on each to learn more.

Entry | Intermediate | Advanced

- You should have familiarity with basic concepts and processes and the ability to apply these with frequent, specific guidance
- You can complete tasks on your own after being told or shown how but require close or frequent guidance
- You should be able to perform successfully in routine, structured situations

Which level is right for you?

Proficiency levels are not tied to a specific grade level or years of experience. The proficiency level required for each Work Role varies by position, career level, and organizational needs. In fact, it's likely you'll find yourself at different proficiency levels for different Work Roles. You and your supervisor have the flexibility to determine which proficiency level is right for you for each Work Role. You'll learn how to do this in the next section.

What are Proficiency Levels?

Proficiency is used to indicate a degree of capability or expertise in a specific Knowledge, Skill, or Ability that allows one to function independently in performing that Knowledge or Skill. Proficiencies also provide a mechanism for organizations to assess learners. Work Roles are composed of Tasks that constitute work to be done; Tasks include associated Knowledge and Skill statements that represent learners' potential to perform those Tasks. Proficiency is not aligned to position level or to pay scale such as the General Schedule (GS) for government employees.

There are three proficiency levels. Click on each to learn more.

Entry | Intermediate | Advanced

- You must have extensive knowledge of basic concepts and processes as well as experience applying these with only periodic high-level guidance
- You must be able to perform successfully in non-routine and sometimes complicated situations
- You are able to draw conclusions and make recommendations

Which level is right for you?

Proficiency levels are not tied to a specific grade level or years of experience. The proficiency level required for each Work Role varies by position, career level, and organizational needs. In fact, it's likely you'll find yourself at different proficiency levels for different Work Roles. You and your supervisor have the flexibility to determine which proficiency level is right for you for each Work Role. You'll learn how to do this in the next section.

What are Proficiency Levels?

Proficiency is used to indicate a degree of capability or expertise in a specific Knowledge, Skill, or Ability that allows one to function independently in performing that Knowledge or Skill. Proficiencies also provide a mechanism for organizations to assess learners. Work Roles are composed of Tasks that constitute work to be done; Tasks include associated Knowledge and Skill statements that represent learners' potential to perform those Tasks. Proficiency is not aligned to position level or to pay scale such as the General Schedule (GS) for government employees.

There are three proficiency levels. Click on each to learn more.

Entry | Intermediate | Advanced

- You must have an in-depth understanding of advanced concepts and processes and experience applying these with little to no guidance
- You must be able to serve as a resource and provide guidance to others
- You must also be able to perform successfully in complex, unstructured situations

Which level is right for you?

Proficiency levels are not tied to a specific grade level or years of experience. The proficiency level required for each Work Role varies by position, career level, and organizational needs. In fact, it's likely you'll find yourself at different proficiency levels for different Work Roles. You and your supervisor have the flexibility to determine which proficiency level is right for you for each Work Role. You'll learn how to do this in the next section.

Charting Your Cybersecurity Career Development Path

Now that you understand the NICE Framework Categories, Specialty Areas, and Work Roles you're ready to chart your career development path. The next few pages walk you through each step.

Step 1

Document the Categories, Specialty Areas, and Work Roles that apply to you

Step 2

Assess your proficiency level for each of your Work Roles

Step 3

Prioritize Work Role areas to target for growth

Step 4

Identify development opportunities that align with your target Work Roles

Step 5

Build your Cybersecurity Training Plan

Charting Your Career Development Path

Step 1: Document the Categories, Specialty Areas, and Work Roles that apply to your position

The first step in charting your career path is to document the NICE Framework areas that apply to you. Review the various levels in the NICE Framework tab to identify the relevant Categories, Specialty Areas, and Work Roles for your position and Agency needs. Understanding the layers of the NICE Framework and how they apply to you will help you dive deeper into creating a career path.

Categories

Seven (7) to choose from

Highest level of the NICE Framework

Specialty Areas

Thirty-three (33) to choose from

Second level of the NICE Framework

Work Roles

Fifty-two (52) to choose from

Third level of the NICE Framework and most detailed

"Your talent is needed to advance the President's commitment to elevate cybersecurity as a top priority across the government, strengthen partnerships with the private sector, and expand our investment in infrastructure and people."

-Alejandro Mayorkas, Secretary of the Department of Homeland Security

Charting Your Career Development Path

Step 2: Assess your proficiency level for each of your Work Roles

For each NICE Framework Work Role that applies to you, select the proficiency level that aligns with your current Tasks and KSAs on the Career Development Planning Worksheet. The level you choose for each area may be different—you may be entry in some areas and intermediate in others. Be sure to honestly assess how well you demonstrate the proficiencies right now. There is no right or wrong answer. Get feedback from your manager to make sure you're both on the same page.

Here's a simple guide to help you accurately assess your proficiency level. Ask yourself where you fall on the continuum for each Work Role. If you feel like you fall in between two levels, make a judgment call on which way you lean or ask your manager to weigh in.

Proficiency Level	Questions to Ask Yourself
Entry	❑ Do I understand only the basic terminology, concepts, and principles related to this competency? ❑ Can I only apply them in simple situations, but struggle in more complicated ones? ❑ Do I often have to seek guidance and support from someone more senior than me?
Intermediate	❑ Do I have a solid understanding of the key terminology, concepts, and principles? ❑ Am I comfortable explaining concepts to others and participating in discussions? ❑ Can I generally perform independently and only seek guidance in complex or difficult situations?
Advanced	❑ Do I have in-depth knowledge of the key terminology, concepts, and principles? ❑ Can I discuss, explain, advise, and debate concepts? ❑ Do others often seek my input and advice as a recognized expert?

Charting Your Career Development Path

Step 3: Prioritize Work Role areas that you want to target for growth

Now that you know which Work Roles apply to your position and what your current proficiencies levels are, you can prioritize the Work Roles. This step ensures your time is invested in improving the proficiency levels that matter most. Here are a few considerations:

- Use CISA's Cyber Career Pathways Tool to:
  - Learn more about the Tasks associated with each Work Role
  - Understand the Knowledge, Skills, and Abilities associated with each Work Role
  - Gain a greater understanding of Capability Indicators and Proficiency Levels
  - View the common relationships between the various Work Roles
- Prioritize Work Roles with the lowest proficiency levels to help you stay focused on the areas that are most in need of growth. Also, prioritize the ones that are most important to your current job. Not all Tasks and KSAs carry the same weight, so target ones that will have the biggest impact.
- If you are early in your career, prioritize new Work Roles or Tasks and KSAs to gain complementary Skills and Knowledge. You may want to develop multiple Work Roles to help you decide the career path you want to take.
- If you are later in your career, you may want to develop new Work Roles, Tasks and KSAs to stay fresh, learn different perspectives, and avoid getting complacent.

Talk to your supervisor to determine which strategy is best for you.

Charting Your Career Development Path

Step 4: Identify development opportunities that align with your target Work Roles

Let's recap:

- You know what Tasks and KSAs apply to your job
- You know your current proficiency level for each
- You know which Work Roles you want to target for growth

Now, you're ready to identify training and professional development opportunities in those areas. This guide has over 150 development activities for you to consider. These opportunities are broken into the following categories.

Professional Development Training are recommended courses offered by CISA that align to the NICE Framework and proficiency levels discussed in this Guide.

Competitions and Games encourage players to practice, hone cybersecurity skills, and build confidence in a controlled, real-world environment.

Certifications are credentials you can earn to validate your skills and knowledge.

Experience Opportunities are development activities beyond formal courses. They include mentoring, rotational assignments, and self-study.

Review the training options on your own and with your manager to select the best ones for you.

Charting Your Career Development Path

Step 5: Build your Cybersecurity Training Plan

The last step is to use all the information you gathered in Steps 1-4 to build your Cybersecurity Training Plan. Creating your plan should be a joint effort between you and your supervisor. Review the available training and professional development opportunities in this Guide together and discuss the best options for you. Talk about the areas you should focus on and make a plan to achieve your career goals.

Since your Cybersecurity Training Plan should capture short- and long-range goals, you can sequence the training and development activities into a roadmap for future growth. Start with your immediate needs and build upon them by planning development activities over the next years.

Building your Cybersecurity Training Plan is only the first step. Your plan is a living document that you should revisit and refresh each year with your supervisor. As you complete trainings and develop your skills throughout the year, you may find your career goals shift or you may uncover new interests. Update your plan each year to make sure it reflects your current direction.

The remainder of this Guide has details on hundreds of training courses, certifications, leadership programs, and other ideas for professional development. With this information, your plan will practically write itself!

CyberPay

The federal government is serious about recruiting and retaining highly skilled cyber professionals.

Check the Office of Personnel Management's Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals guide to see how to qualify for incentives offered to cyber professionals working in the federal government.

Professional Development Training

◄ Prev Next ►

Training is an excellent way to improve work performance, gain new Knowledge, Skills and Abilities, and make positive strides in your personal and professional development. Use the matrix on the following pages to determine the courses that align with your targeted Work Roles and proficiency levels. All of the courses listed in the matrix are provided by CISA. Click on each course title to learn more. Record the trainings you would like to take for discussion with your manager and inclusion in your Cybersecurity Training Plan.

Here are a few tips to help you make the most of the training matrix:

- **Courses are grouped by NICE Framework Category:** use the Navigation Menu at the top to jump to different courses for each Category
- Use CISA's Cyber Career Pathways Tool to review the Tasks and KSAs for the Work Roles you're targeting for growth
- The courses listed in this Guide are free at anytime and are almost all self-paced

Note on Training

The course list on the following pages are all provided by CISA and there are many alternatives available. If you don't find what you're looking for, talk to your supervisor about other options or check back for updates to this Guide.

When you click on the course titles to learn more, some sites will bring you directly to the course registration page and others may prompt you to log in first.

Professional Development Training

◄ Prev Next ►

To get the most out of this matrix, review the descriptions below before you get started.

Course titles are hyperlinked for easy access

Brief description of what you'll learn

Find the course that's right for you

Degree of difficulty of the course

All courses are mapped to the NICE Framework

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Collect and Operate	
				Specialty Areas	Work Roles
IMR 002 – Cloud Security	The course includes an overview of cloud-based environment attacks and how threat actors compromise systems to damage operations, escalate privileges, and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT, Veterans	Entry	3	3

Icons represent the number of SA and WR each course has. Hover your cursor over the number to see what they are.

All-Source Analysis, Exploitation Analysis, Threat Analysis

Mission Assessment Specialist, Exploitation Analyst, Threat/Warning Analyst

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
Creating a Computer Security Incident Response Team (CSIRT)	This course is for organizations and individuals who are at the beginning of their planning and implementation process for creating a computer security incident response team or an incident management capability.	Federal, SLTT, Veterans	Entry	1	1
Cyber Fundamentals for Law Enforcement Investigations	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.	Federal, SLTT, Veterans	Entry	1	1
Don't Wake Up to a Ransomware Attack	This course provides essential knowledge and reviews real-life examples of these attacks to help you and your organization to prevent, mitigate, and respond to the ever-evolving threat of ransomware.	Federal, SLTT, Veterans	Entry	3	3

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
Foundations of Incident Management	This course introduces 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.	Federal, SLTT, Veterans	Entry	1	1
Hacker 101 and Secure Coding	This course is designed to introduce students to the basic concepts of hacker activity, understand how to combat such activities, and learn how to reduce the risk of cyber-attacks by understanding the hacker mindset. The course covers reconnaissance before a hacker attack, exploiting a system and performing an attack, and post-exploit activities.	Federal, SLTT, Veterans, Public	Entry	1	1
IMR 001 - Ransomware	The course includes an overview of ransomware attacks and how threat actors compromise systems to lock out legitimate users and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	3	3

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
IMR 002 – Cloud Security	The course includes an overview of cloud-based environment attacks and how threat actors compromise systems to damage operations, escalate privileges, and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	3	3
IMR 003 – Business Email Compromise	This course puts you front and center for a live, two-hour red team/blue team cyber range demonstration of a Business Email Compromise cyberattack. Be in the room where it happens, guided by expert engineers through the attack and defense strategy of each side to impart understanding and essential takeaways that prepare you and your organization for what it takes to orchestrate an effective response to a real-time cyberattack.	Federal, SLTT	Entry	3	3
IMR 102 – Cloud-based Server Attacks: Don't Get Caught in the Storm	An overview of cloud computing and its associated security vulnerabilities, common signs of a cloud server attack and how to respond to suspicious activity, CISA guidance and best practices to mitigate cloud server vulnerabilities, secure cloud systems, and block threat activity, case studies demonstrating the impacts of cloud attacks, including major data breaches	Federal, SLTT	Entry	2	2

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
IMR 103 – Business Email Compromise: Preventing Business Email Attacks	An overview of business email compromise, phishing, and its impact on organizations. Learn how to identify a business email attack, mitigate the likelihood and impact of BEC through best practices, and respond and recover funds in the event of an attack.	Federal, SLTT	Entry	1	1
IMR 104 – Internet-Accessible System Vulnerabilities: Don't Let Cyber Criminals Steal Your Connections	Internet-accessible systems have become the backbone of modern business and communication infrastructure, from smartphones to web applications such as Outlook to the explosive growth of the "Internet of Things" (IoT). Each of these systems and devices, however, can be targeted by threat actors and used to conduct malicious activity if they are unsecured.	Federal, SLTT	Entry	1	1
IMR 106 – DNS Infrastructure Tampering: Strengthen Your Resolve	Understand DNS and its vulnerabilities: Learn how the Domain Name System works, and how threat actors target its vulnerabilities to conduct malicious activity. Identify signs of a DNS attack: Understand common red flags that indicate potential attack, and how to verify suspicious activity. Receive CISA guidance and best practices: Review official CISA guidance to help organizations prevent, mitigate, and recover from DNS attacks.	Federal, SLTT	Entry	2	2

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
IMR 107 – High-Value Assets	Define high value assets, and how to assess and prioritize risks. Understand the most likely threats to HVAs and how to mitigate associated vulnerabilities. Learn the steps and parameters to identify, categorize, prioritize, and secure your HVAs or critical assets. Explore the impacts of documented critical or high value asset cyberattacks, and the success of resulting response and recovery efforts.	Federal, SLTT	Entry	1	1
Introduction to Computer Forensics	This course introduces the tasks, processes, and technologies to identify, collect and preserve, and analyze data so that it can be used in a judiciary setting. The course begins with obtaining and imaging data and then describes each step in following the forensic process.	Federal, SLTT, Veterans	Entry	1	1
Introduction to Cyber Intelligence	This course provides an introduction into a Cyber Intelligence Conceptual Framework and explores intelligence tradecraft fundamentals from information gathering, data validation, analysis and communication. Students will learn how cyber intelligence differs from cybersecurity and cyber threat intelligence.	Federal, SLTT, Veterans	Entry	2	2

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
Introduction to Threat Hunting Teams	This course provides basic definitions, activities, and examples of teams hunting threats in the cyber domain. Content covers how hunting teams establish goals, methods used by threat hunting teams, and sources available to help read and interpret the threat landscape.	Federal, SLTT, Veterans	Entry	1	1
Overview of Creating and Managing Computer Security Incident Response Teams (CSIRTs)	This course is designed to provide the learner with an overview of what is needed to create and operate a Computer Security Incident Response Team (CSIRT). Topics covered within the course include the benefits and limitations of a CSIRT, CSIRT requirements, services, common policies and procedures, and operational best practices.	Federal, SLTT, Veterans	Entry	1	1
Understanding DNS Attacks	This course provides key information you need to know to protect yourself and your organization from DNS infrastructure tampering including common vulnerabilities, how to identify a potential attack, and guidance and best practices to mitigate the likelihood and impact of a successful DNS attack.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
Understanding Web and Email Server Security	Enable learners to prevent, flag, and protect themselves and their organizations from web and email server cyberattacks through awareness of common attack schemes, best practices, CISA guidance, and resources.	Federal, SLTT, Veterans	Entry	2	2
201 Intermediate Cybersecurity for Industrial Control Systems, Part 1	This course provides technical instruction on the protection of Industrial Control Systems using offensive and defensive methods. Attendees will recognize how cyber attacks are launched, why they work, and mitigation strategies to increase the cybersecurity posture of their Control System networks. This course acts as a prerequisite for the next course, Intermediate Cybersecurity for Industrial Control Systems (202).	Federal, SLTT, Veterans	Intermediate	1	1
202 Intermediate Cybersecurity for Industrial Control Systems, Part 2	This course provides a brief review of ICS security including a comparative analysis of IT and control system architectures, security vulnerabilities, and mitigation strategies unique to the Control System domain. Accompanying this course is a sample Process Control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions. This network is also used during the course for the hands-on exercises.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
Advanced PCAP Analysis and Signature Development	The Advanced PCAP Analysis and Signature Development (APA) course takes users through an introduction to rules, goes over example syntax, protocols and expressions. This course contains several supporting video demonstrations as well as lab exercises writing and testing basic rules.	Federal, SLTT, Veterans	Intermediate	1	1
Attack Methodologies in IT & ICS (210W-09)	Understand how hackers attack systems helps you better understand how to defend against cyber attacks.	Federal, SLTT	Intermediate	3	3
Current Trends (Threat) (210W-06)	Risk is a function of threat, vulnerability, and consequence. The most complex attribute is threat because it can be intentional or unintentional, natural or man-made. When trying to develop defensive strategies to protect controls systems, it is important to understand the threat landscape in order for appropriate countermeasures or compensating controls to be deployed.	Federal, SLTT	Intermediate	2	2

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
Current Trends (Vulnerabilities) (210W-07)	In this course, we examine some of the current trends in cybersecurity vulnerabilities that contribute directly to cyber risk in Industrial Control Systems (ICSs). The goal is to identify the root causes and their associated countermeasures that can be used to protect control systems.	Federal, SLTT	Intermediate	1	1
Cyber Supply Chain Risk Management	This course focuses on cyber supply chain risk management, also known as C-SCRM, and the role it plays within our society today. This course will explain how to securely provision, analyze, oversee and govern, protect and defend a supply chain.	Federal, SLTT, Veterans, Public	Intermediate	4	5
Cybersecurity Analyst	The Cybersecurity Analyst course is designed to help reinforce concepts that require monitoring and information analysis to respond to suspicious events. This intermediate-level course focuses on defense techniques leveraging data and tools to identify risks to an organization and apply effective mitigation strategies to detect and respond to threats.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
Cybersecurity Risk (210W-05)	This course is designed to help you gain a better understanding of cyber risk, how it is defined in the context of ICS security, and the factors that contribute to risk. This will empower you to develop cybersecurity strategies that align directly with the ICS environment. Also, learn how IT-based countermeasures can be customized to accommodate for the uniqueness of ICS architectures.	Federal, SLTT	Intermediate	2	2
Emerging Cyber Security Threats	This course covers a broad range of cybersecurity elements that pose threats to information security posture such as 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.	Federal, SLTT, Veterans	Intermediate	1	1
Enterprise Cybersecurity Operations	This course highlights technical knowledge and skills required for implementing secure solutions in the enterprise. A broad spectrum of disciplines is covered to aid practitioners in applying frameworks and controls to improve the security posture while supporting the business mission.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
ICS Cybersecurity Consequences (210W-08)	A cyber attack that results in the release of a toxic chemical and kills 10 people is more significant than a cyber attack that temporarily disables the HVAC in a control – or is it? This course will help you better understand the impacts of cyber based attack can have on an ICS and provide you with different ways of looking at the potential consequences of three types of events.	Federal, SLTT	Intermediate	1	1
IMR 204 – Vulnerabilities of Internet-Accessible Systems: Defending Internet-Accessible Systems Cyber Range Training	Four activities that explore the following aspects: network mapping, identifying and remediating vulnerabilities in internet-accessible systems, and resolving password spraying attacks. Participants will use tools and work with cybersecurity engineers in a host environment with a sample hygiene assessment report to investigate the network, prioritize vulnerabilities, and apply firewall rules to your network.	Federal, SLTT	Intermediate	1	1
IMR 205 – Web and Email Server Attacks	Participants will be introduced to common web and email vulnerabilities, as well as the technologies of encryption and authentication to enhance web and email security. This exercise uses a hands-on approach to facilitate realistic technical training and interaction opportunities for learners.	Federal, SLTT	Intermediate	2	2

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
IMR 206 – DNS Infrastructure Attacks	Working with cybersecurity engineers in a host environment with various software applications, participants will be introduced to common DNS tampering techniques, as well as the technologies of DNS sinkholing to enhance security. Learners will analyze network and host-based artifacts and implement remediation for the identified vulnerabilities.	Federal, SLTT	Intermediate	2	2
Insider Threat Analysis	This course is designed to help insider threat analysts understand data that can be used to prevent, detect, and respond to insider threats by working with data from multiple sources to develop indicators of potential insider activity, as well as strategies for developing and implementing an insider threat analysis and response.	Federal, SLTT, Veterans	Intermediate	1	1
Insider Threat Program Manager: Implementation and Operations	This course discusses various techniques and methods to develop, implement, and operate program components. The content covered supports organizations implementing and managing insider threat detection and prevention programs based on various government mandates or guidance.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
Mapping IT Defense-in-Depth Security Solutions to ICS, Part 2	This training will continue the defense-in-depth model and cover layer 3 - Network Security.	Federal, SLTT	Intermediate	1	1
Root Cause Analysis	This course provides an explanation of root cause analysis for cyber security incidents and an overview of two different root cause analysis models (and approaches used in these models). The course describes how root cause analysis can benefit other incident management processes (response, prevention, and detection), and details general techniques that can be adopted as methods for analysis of cyber incidents.	Federal, SLTT, Veterans	Intermediate	1	1
301 ICS Cybersecurity	This course provides extensive hands-on training on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber attacks. Trainees will learn about common vulnerabilities and the importance of understanding the environment they are tasked to protect. Learning the weaknesses of a system will enable trainees to implement the mitigation strategies and institute policies and programs that will provide the defense-in-depth needed to ensure a more secure ICS environment.	Federal, SLTT	Advanced	1	1

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
401 ICS Evaluation	This instructor-led 5-day course provides hands-on training on how to analyze, evaluate, and document the cybersecurity posture of an organization's Industrial Control Systems (ICS) for the purpose of identifying recommended changes. Specifically, the course will utilize a multi-step repeatable process, within a simulated ICS environment, that teaches how to analyze cybersecurity weaknesses and threats, evaluate and map findings, document potential mitigations, and provide ongoing resolutions to strengthen the cybersecurity posture.	Federal, SLTT	Advanced	3	3
Advanced Computer Forensics	This course focuses on building skills to improve the ability to piece together the various components of the digital investigation. The course begins with acquisition planning and preparation, progresses through the investigative process, and concludes with analysis techniques and methods for more manageable investigations.	Federal, SLTT, Veterans	Advanced	1	1
IMR 302 – Cloud Leak: Cloud Leak Cyber Range Challenge	Scenario: Participants must capture network and host-based artifacts from the attack, report the source and extent of a compromise, and provide recommendations for hardening the network against attack and better data hygiene practices.	Federal, SLTT	Advanced	2	2

Professional Development Training

◄ Prev Next ►

Analyze

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Analyze	
				Specialty Areas	Work Roles
IMR 303 - Business Email Attack: Business Email Compromise Cyber Range Challenge	Scenario: Your organization receives an announcement that a Business Email Compromise is suspected to have occurred. Participants then use tools on the host environment to investigate the intrusion and uncover evidence. Once data collection is complete, participants submit a briefing and discuss their findings.	Federal, SLTT	Advanced	2	2

Professional Development Training

◄ Prev Next ►

Collect and Operate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Collect and Operate – Specialty Areas	NICE Framework Mapping: Collect and Operate – Work Roles
Cyber Security Investigations	This course discusses the basic concepts of cybersecurity and digital forensics investigation practices such as performing collection and triage of digital evidence in response to an incident, evidence collection methodologies, and forensic best practices. This course defines what assumptions are, describes how different kinds of assumptions may be challenged, and covers the importance of seeking out other people's perspectives.	Federal, SLTT, Veterans	Entry	1	1
Don't Wake Up to a Ransomware Attack	This course provides essential knowledge and reviews real-life examples of these attacks to help you and your organization to prevent, mitigate, and respond to the ever-evolving threat of ransomware.	Federal, SLTT, Veterans	Entry	1	2
Foundations of Cybersecurity for Managers	This course is designed for managers and other stakeholders who may be involved in decision making that would include considerations for security in a cyber environment but do not have a strong technical background. The course aims to help the learner better understand how people and technology work together to protect mission critical assets, and the frameworks leveraged to assess and apply security controls.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Collect and Operate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Collect and Operate	
				Specialty Areas	Work Roles
IMR 001 - Ransomware	This course includes an overview of ransomware attacks and how threat actors compromise systems to lock out legitimate users and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	1	2
IMR 002 - Cloud Security	This course includes an overview of cloud-based environment attacks and how threat actors compromise systems to damage operations, escalate privileges, and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	1	2
IMR 003 - Business Email Compromise	This course puts you front and center for a live, two-hour red team/ blue team cyber range demonstration of a Business Email Compromise cyberattack. Be in the room where it happens, guided by expert engineers through the attack and defense strategy of each side to impart understanding and essential takeaways that prepare you and your organization for what it takes to orchestrate an effective response to a real-time cyberattack.	Federal, SLTT	Entry	1	2

Professional Development Training

◄ Prev Next ►

Collect and Operate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Collect and Operate – Specialty Areas	NICE Framework Mapping: Collect and Operate – Work Roles
IMR 102 - Cloud-based server attacks: Don't Get Caught in the Storm	An overview of cloud computing and its associated security vulnerabilities, common signs of a cloud server attack and how to respond to suspicious activity, CISA guidance and best practices to mitigate cloud server vulnerabilities, secure cloud systems, and block threat activity, case studies demonstrating the impacts of cloud attacks, including major data breaches	Federal, SLTT	Entry	1	2
IMR 103 - Business Email Compromise: Preventing Business Email Attacks	An overview of business email compromise, phishing, and its impact on organizations. Learn how to identify a business email attack, mitigate the likelihood and impact of BEC through best practices, and respond and recover funds in the event of an attack.	Federal, SLTT	Entry	1	2
IMR 104 - Internet-Accessible System Vulnerabilities: Don't Let Cyber Criminals Steal Your Connections	Internet-accessible systems have become the backbone of modern business and communication infrastructure, from smartphones to web applications such as Outlook to the explosive growth of the "Internet of Things" (IoT). Each of these systems and devices, however, can be targeted by threat actors and used to conduct malicious activity if they are unsecured.	Federal, SLTT	Entry	1	2

Professional Development Training

◄ Prev Next ►

Collect and Operate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Collect and Operate	
				Specialty Areas	Work Roles
IMR 106 - DNS Infrastructure Tampering: Strengthen Your Resolve	Learn how the Domain Name System works, and how threat actors target its vulnerabilities to conduct malicious activity. Identify signs of a DNS attack, understand common red flags that indicate a potential attack, and how to verify suspicious activity. Receive CISA guidance and best practices to help organizations prevent, mitigate, and recover from DNS attacks.	Federal, SLTT	Entry	2	5
IMR 107 - High-Value Assets	Define high value assets, and how to assess and prioritize risks. Understand the most likely threats to HVAs and how to mitigate associated vulnerabilities. Learn the steps and parameters to identify, categorize, prioritize, and secure your HVAs or critical assets. Explore the impacts of documented critical or high value asset cyberattacks, and the success of resulting response and recovery efforts.	Federal, SLTT	Entry	1	2
Measuring What Matters: Security Metrics Workshop	This workshop focuses on how to measure the right things in order to make informed management decisions, take the appropriate actions, and change behaviors. Students will learn how to refine a strategic or business objective that meets that S.M.A.R.T.E.R. criteria: Specific, Measurable, Achievable, Relevant, Time-bound, Evaluated, Reviewed, and can be used to initiate the Goal - Question - Indicator - Metric (GQIM) process.	Federal, SLTT	Entry	1	1

Professional Development Training

◄ Prev Next ►

Collect and Operate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Collect and Operate	
				Specialty Areas	Work Roles
Overview of Creating and Managing Computer Security Incident Response Teams (CSIRTs)	The Overview of Creating and Managing CSIRTs course is designed to provide the learner with an overview of what is needed to create and operate a Computer Security Incident Response Team (CSIRT). The intended audience is individuals tasked with creating a CSIRT and those who may be new to CSIRT issues and processes. Topics covered within the course include the benefits and limitations of a CSIRT, CSIRT requirements, services, common policies and procedures, and operational best practices.	Federal, SLTT, Veterans	Entry	1	1
Understanding DNS Attacks	This course provides key information you need to know to protect yourself and your organization from DNS infrastructure tampering including common vulnerabilities, how to identify a potential attack, and guidance and best practices to mitigate the likelihood and impact of a successful DNS attack.	Federal, SLTT, Veterans	Entry	1	2
Understanding Web and Email Server Security	Understanding Web and Email Server Security	Federal, SLTT, Veterans	Entry	2	5

Professional Development Training

◄ Prev Next ►

Collect and Operate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Collect and Operate	
				Specialty Areas	Work Roles
Advanced PCAP Analysis and Signature Dev	The Advanced PCAP Analysis and Signature Development (APA) course takes users through an introduction to rules, goes over example syntax, protocols and expressions. This course contains several supporting video demonstrations as well as lab exercises writing and testing basic rules.	Federal, SLTT, Veterans	Intermediate	1	1
Analysis Pipeline	This course is designed for network flow data analysts who use or are considering using Analysis Pipeline (http://tools.netsa.cert.org/analysis-pipeline5/index.html) as well as cybersecurity researchers. The course aims to help students 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.	Federal, SLTT, Veterans	Intermediate	1	1
Artificial Intelligence (AI) and Machine Learning (ML) for Cyber	The AI/ML for Cyber course is designed to provide students with an overview of the foundational practices and ethical principles of Artificial Intelligence such as reducing risk and unwanted bias to create ethical, transparent, and fair artificial intelligence systems.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Collect and Operate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Collect and Operate	
				Specialty Areas	Work Roles
Cyber Dark Arts	This course highlights 'dark' or deceptive activities employed by malicious users via the Internet as well as topics such as zero-day attacks, dark web, alternate OSs, VPN/TOR, weaponized psychology, and anonymous services.	Federal, SLTT, Veterans, Public	Intermediate	1	1
Differences in Deployments of Industrial Control Systems (210W-01)	This course discusses what, where, and how industrial control systems (ICSs) are used and describes some of specific examples of how ICSs work in real-life situations.	Federal, SLTT	Intermediate	1	1
Enterprise Cybersecurity Operations	This course highlights technical knowledge and skills required for implementing secure solutions in the enterprise. A broad spectrum of disciplines is covered to aid practitioners in applying frameworks and controls to improve the security posture while supporting the business mission.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Collect and Operate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Collect and Operate	
				Specialty Areas	Work Roles
IMR 205 - Web and Email Server Attacks	Participants will be introduced to common web and email vulnerabilities, as well as the technologies of encryption and authentication to enhance web and email security. This exercise uses a hands-on approach to facilitate realistic technical training and interaction opportunities for learners.	Federal, SLTT	Intermediate	2	5
IMR 206 - DNS Infrastructure Attacks	Working with cybersecurity engineers in a host environment with various software applications, participants will be introduced to common DNS tampering techniques, as well as the technologies of DNS sinkholing to enhance security. Learners will analyze network and host-based artifacts and implement remediation for the identified vulnerabilities.	Federal, SLTT	Intermediate	1	2
Mapping IT Defense-in-Depth Security Solutions to ICS, Part 2	This training will continue the defense-in-depth model and cover layer 3 - Network Security.	Federal, SLTT	Intermediate	1	3

Professional Development Training

◄ Prev Next ►

Collect and Operate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Collect and Operate	
				Specialty Areas	Work Roles.
Securing Infrastructure Devices	This course covers physical security, operating system security, management traffic security, device service hardening, securing management services and device access privileges.	Federal, SLTT, Veterans	Intermediate	1	1
(ISC)² ™ CISSP Concentration: ISSEP	This course focuses on applying security and systems engineering principles into business functions to help students prepare to sit for the specialized (ISSEP) certification exam.	Federal, SLTT, Veterans	Advanced	1	1
401 ICS Evaluation	This instructor-led 5-day course provides hands-on training on how to analyze, evaluate, and document the cybersecurity posture of an organization's Industrial Control Systems (ICS) for the purpose of identifying recommended changes. Specifically, the course will utilize a multi-step repeatable process, within a simulated ICS environment, that teaches how to analyze cybersecurity weaknesses and threats, evaluate and map findings, document potential mitigations, and provide ongoing resolutions to strengthen the cybersecurity posture.	Federal, SLTT	Advanced	1	1

Professional Development Training

◄ Prev Next ►

Collect and Operate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Collect and Operate	
				Specialty Areas	Work Roles
IMR 302 - Cloud Leak: Cloud Leak Cyber Range Challenge	Scenario: Participants must capture network and host-based artifacts from the attack, report the source and extent of a compromise, and provide recommendations for hardening the network against attack and better data hygiene practices.	Federal, SLTT	Advanced	1	2
IMR 303 - Business Email Attack: Business Email Compromise Cyber Range Challenge	Scenario: Your organization receives an announcement that a Business Email Compromise is suspected to have occurred. Participants then use tools on the host environment to investigate the intrusion and uncover evidence. Once data collection is complete, participants submit a briefing and discuss their findings.	Federal, SLTT	Advanced	1	2

Professional Development Training

◄ Prev Next ►

Investigate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Investigate	
				Specialty Areas	Work Roles
Cryptocurrency for Law Enforcement	This course covers the history, risks, and legality of cryptocurrency as well as discusses what cryptocurrency items can be seized by law enforcement.	Federal, SLTT, Veterans	Entry	2	2
Cyber Fundamentals for Law Enforcement Investigations	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.	Federal, SLTT, Veterans	Entry	2	2
Cyber Security Investigations	This course discusses the basic concepts of cybersecurity and digital forensics investigation practices such as performing collection and triage of digital evidence in response to an incident, evidence collection methodologies, and forensic best practices.	Federal, SLTT, Veterans	Entry	2	2

Professional Development Training

◄ Prev Next ►

Investigate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Investigate – Specialty Areas	NICE Framework Mapping: Investigate – Work Roles
Don't Wake Up to a Ransomware Attack	This course provides essential knowledge and reviews real-life examples of these attacks to help you and your organization to prevent, mitigate, and respond to the ever-evolving threat of ransomware.	Federal, SLTT, Veterans	Entry	1	2
IMR 001 - Ransomware	The course includes an overview of ransomware attacks and how threat actors compromise systems to lock out legitimate users and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	1	2
IMR 002 - Cloud Security	The course includes an overview of cloud-based environment attacks and how threat actors compromise systems to damage operations, escalate privileges, and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	1	2

Professional Development Training

◄ Prev Next ►

Investigate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Investigate	
				Specialty Areas	Work Roles
IMR 003 - Business Email Compromise	This course puts you front and center for a live, two-hour red team/ blue team cyber range demonstration of a Business Email Compromise cyberattack. Be in the room where it happens, guided by expert engineers through the attack and defense strategy of each side to impart understanding and essential takeaways that prepare you and your organization for what it takes to orchestrate an effective response to a real-time cyberattack.	Federal, SLTT	Entry	1	2
Introduction to Computer Forensics	This course introduces the tasks, processes, and technologies to identify, collect and preserve, and analyze data so that it can be used in a judiciary setting. The course begins with obtaining and imaging data and then describes each step in following the forensic process.	Federal, SLTT, Veterans	Entry	1	1
Introduction to Cyber Intelligence	The course provides an introduction into a Cyber Intelligence Conceptual Framework and explores intelligence tradecraft fundamentals from information gathering, data validation, analysis and communication. Students will learn how cyber intelligence differs from cybersecurity and cyber threat intelligence.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Investigate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Investigate	
				Specialty Areas	Work Roles
Introduction to Investigation of Digital Assets	This course provides an overview of the digital investigation process and key activities performed throughout the process.	Federal, SLTT, Veterans	Entry	2	2
Mobile and Device Security	This 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.	Federal, SLTT, Veterans	Entry	1	1
IMR 204 - Vulnerabilities of Internet-Accessible Systems: Defending Internet-Accessible Systems Cyber Range Training	Four activities that explore the following aspects: network mapping, identifying and remediating vulnerabilities in internet-accessible systems, and resolving password spraying attacks. Participants will use tools and work with cybersecurity engineers in a host environment with a sample hygiene assessment report to investigate the network, prioritize vulnerabilities, and apply firewall rules to your network.	Federal, SLTT	Intermediate	1	2

Professional Development Training

◄ Prev Next ►

Investigate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Investigate	
				Specialty Areas	Work Roles
IMR 205 - Web and Email Server Attacks	Participants will be introduced to common web and email vulnerabilities, as well as the technologies of encryption and authentication to enhance web and email security. This exercise uses a hands-on approach to facilitate realistic technical training and interaction opportunities for learners.	Federal, SLTT	Intermediate	1	2
IMR 206 - DNS Infrastructure Attacks	Working with cybersecurity engineers in a host environment with various software applications, participants will be introduced to common DNS tampering techniques, as well as the technologies of DNS sinkholing to enhance security. Learners will analyze network and host-based artifacts and implement remediation for the identified vulnerabilities.	Federal, SLTT	Intermediate	1	2
Securing The Network Perimeter	This course covers edge security traffic design, blocking DoS/DDoS traffic, specialized access control lists, routers and firewalls, securing routing protocols, securing traffic prioritization and securing against SPOF.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Investigate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Investigate	
				Specialty Areas	Work Roles
Advanced Computer Forensics	This course focuses on building skills to improve the ability to piece together the various components of the digital investigation. The course begins with acquisition planning and preparation, progresses through the investigative process, and concludes with analysis techniques and methods for more manageable investigations.	Federal, SLTT, Veterans	Advanced	1	1
IMR 302 - Cloud Leak: Cloud Leak Cyber Range Challenge	Scenario: Participants must capture network and host-based artifacts from the attack, report the source and extent of a compromise, and provide recommendations for hardening the network against attack and better data hygiene practices.	Federal, SLTT	Advanced	1	2
IMR 303 - Business Email Attack: Business Email Compromise Cyber Range Challenge	Scenario: Your organization receives an announcement that a Business Email Compromise is suspected to have occurred. Participants then use tools on the host environment to investigate the intrusion and uncover evidence. Once data collection is complete, participants submit a briefing and discuss their findings.	Federal, SLTT	Advanced	1	2

Professional Development Training

◄ Prev Next ►

Investigate

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Investigate	
				Specialty Areas	Work Roles
Mobile Forensics	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.	Federal, SLTT, Veterans	Advanced	2	2

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
(ISC)² ™ Systems Security Certified Practitioner	This course serves as a preparation for the Systems Security Certified Practitioner (SSCP) certification exam, by demonstrating advanced technical skills and knowledge required to implement and administer infrastructure using security best practices, policies, and procedures.	Federal, SLTT, Veterans	Entry	2	2
101 Introduction to Control Systems Cybersecurity	This course introduces students to the basics of ICS cybersecurity. This includes a comparative analysis of IT and ICS architectures, understanding risk in terms of consequence, security vulnerabilities within ICS environments, and effective cyber risk mitigation strategies for the Control System domain.	Federal, SLTT	Entry	1	1
Advanced Windows Scripting	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.	Federal, SLTT, Veterans	Entry	3	3

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Application and OS Security	The CompTIA A+ 1002 certification prep course is a self-study resource to help students prepare for the CompTIA A+ certification exam, covering topics like installing and configuring operating systems, expanded security, software troubleshooting and operational procedures.	Federal, SLTT, Veterans	Entry	3	3
CDM 141 – Introduction to the New CDM Agency Dashboard	This course provides participants with the essential knowledge of the ES-2 version of the CDM Agency Dashboard. It explains basic features and navigation within the environment, and includes demonstrations using the new CDM Agency Dashboard to identify and report on vulnerabilities.	Federal, SLTT, Veterans	Entry	2	2
CDM 143 – Vulnerability Management with the CDM Agency Dashboard	This course introduces participants to CDM Agency-Wide Adaptive Risk Enumeration (AWARE) and other vulnerability management topics. With the information provided, dashboard users can identify the most critical vulnerabilities and prioritize mitigation activities at their agency.	Federal, SLTT, Veterans	Entry	2	2

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Cloud Security – What Leaders Need to Know	This course features National Defense University Professor Robert Richardson who discusses important security and oversight requirements for commercial cloud solutions.	Federal, SLTT, Veterans, Public	Entry	3	3
Critical Infrastructure Protection	This course discusses 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.	Federal, SLTT, Veterans, Public	Entry	4	4
Cyber Awareness Challenge 2019	This course provides an overview of cybersecurity threats and best practices. Every year, authorized users of certain information systems must complete the Cyber Awareness Challenge to maintain awareness of and stay current on new cybersecurity threats.	Federal, SLTT, Veterans	Entry	N/A	N/A

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Cybersecurity for Technical Staff	This course highlights topics such as risk management, architecture and design, and tools and technologies as well as key concepts for detecting, protecting, and defending from security threats.	Federal, SLTT, Veterans	Entry	3	3
Device Security	This certification prep course is a self-study resource to help students prepare for the CompTIA A+ certification exam, covering topics like mobile devices, networking technology, hardware, virtualization and cloud computing, and network troubleshooting.	Federal, SLTT, Veterans	Entry	3	3
Don't Wake Up to a Ransomware Attack	This course provides essential knowledge and reviews real-life examples of these attacks to help you and your organization to prevent, mitigate, and respond to the ever-evolving threat of ransomware.	Federal, SLTT, Veterans	Entry	6	7

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
IMR 001 – Ransomware	The course includes an overview of ransomware attacks and how threat actors compromise systems to lock out legitimate users and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	6	7
IMR 002 – Cloud Security	The course includes an overview of cloud-based environment attacks and how threat actors compromise systems to damage operations, escalate privileges, and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	6	7
IMR 003 – Business Email Compromise	This course puts you front and center for a live, two-hour red team/ blue team cyber range demonstration of a Business Email Compromise cyberattack. Be in the room where it happens, guided by expert engineers through the attack and defense strategy of each side to impart understanding and essential takeaways that prepare you and your organization for what it takes to orchestrate an effective response to a real-time cyberattack.	Federal, SLTT	Entry	5	6

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
IMR 102 – Cloud-based server attacks: Don't Get Caught in the Storm	An overview of cloud computing and its associated security vulnerabilities, common signs of a cloud server attack and how to respond to suspicious activity, CISA guidance and best practices to mitigate cloud server vulnerabilities, secure cloud systems, and block threat activity, case studies demonstrating the impacts of cloud attacks, including major data breaches	Federal, SLTT	Entry	6	7
IMR 103 - Business Email Compromise: Preventing Business Email Attacks	An overview of business email compromise, phishing, and its impact on organizations. Learn how to identify a business email attack, mitigate the likelihood and impact of BEC through best practices, and respond and recover funds in the event of an attack.	Federal, SLTT	Entry	4	4
IMR 104 - Internet-Accessible System Vulnerabilities: Don't Let Cyber Criminals Steal Your Connections	Internet-accessible systems have become the backbone of modern business and communication infrastructure, from smartphones to web applications such as Outlook to the explosive growth of the "Internet of Things" (IoT). Each of these systems and devices, however, can be targeted by threat actors and used to conduct malicious activity if they are unsecured.	Federal, SLTT	Entry	4	4

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
IMR 105 - Web and Email Server Attacks: Securing Web and Email Servers	Web and email servers are the workhorses of the Internet: we couldn't run government, businesses, or our personal lives without them! However, the information exchanged through web and email servers can offer a tempting target for cyber attackers. Key Guidance for Organizations: CISA provides resources and best practices to help individuals and organizations secure their web and email infrastructure.	Federal, SLTT	Entry	3	4
IMR 106 - DNS Infrastructure Tampering: Strengthen Your Resolve	Understand DNS and its vulnerabilities: Learn how the Domain Name System works, and how threat actors target its vulnerabilities to conduct malicious activity. Identify signs of a DNS attack: Understand common red flags that indicate potential attack, and how to verify suspicious activity. Receive CISA guidance and best practices: Review official CISA guidance to help organizations prevent, mitigate, and recover from DNS attacks.	Federal, SLTT	Entry	5	6
IMR 107 - High-Value Assets	Define high value assets, and how to assess and prioritize risks. Understand the most likely threats to HVAs and how to mitigate associated vulnerabilities. Learn the steps and parameters to identify, categorize, prioritize, and secure your HVAs or critical assets. Explore the impacts of documented critical or high value asset cyberattacks, and the success of resulting response and recovery efforts.	Federal, SLTT	Entry	5	6

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Introduction to Windows Scripting	This course focuses on writing scripts for the Microsoft Windows operating system and covers fundamentals and syntax for automating administrative and security monitoring tasks.	Federal, SLTT, Veterans	Entry	3	3
LAN Security Using Switch Features	Students will learn different methods of how to secure Local Area Networks (LANs) at the connectivity level. Topics include monitoring MAC addresses and port security, limiting MAC & IP spoofing, controlling traffic flows, implementing and enhancing security in VLANs, enabling authentication on connection points, and determining host security health.	Federal, SLTT, Veterans	Entry	2	2
Mobile and Device Security	This 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.	Federal, SLTT, Veterans	Entry	2	2

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Network Layer 1 & 2 Troubleshooting	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.	Federal, SLTT, Veterans	Entry	3	3
Offensive and Defensive Network Operations	This course focuses on fundamental concepts for offensive and defensive network operations such as how 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.	Federal, SLTT, Veterans	Entry	1	1
Securing Internet-Accessible Systems	This course explains the vulnerabilities of internet-accessible systems and how to prepare for, mitigate, and respond to a potential attack. This course provides key knowledge to inform organizational awareness of internet-accessible system attacks as well as best practices that minimize the likelihood of a successful attack and enable effective response and recovery if an attack occurs.	Federal, SLTT, Veterans	Entry	3	4

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Understanding DNS Attacks	This course provides key information you need to know to protect yourself and your organization from DNS infrastructure tampering including common vulnerabilities, how to identify a potential attack, and guidance and best practices to mitigate the likelihood and impact of a successful DNS attack.	Federal, SLTT, Veterans	Entry	5	6
Understanding Web and Email Server Security	Enable learners to prevent, flag, and protect themselves and their organizations from web and email server cyberattacks through awareness of common attack schemes, best practices, CISA guidance, and resources.	Federal, SLTT, Veterans	Entry	5	6
201 Intermediate Cybersecurity for Industrial Control Systems, Part 1	This course provides technical instruction on the protection of Industrial Control Systems using offensive and defensive methods. Attendees will recognize how cyber attacks are launched, why they work, and mitigation strategies to increase the cybersecurity posture of their Control System networks. This course acts as a prerequisite for the next course, Intermediate Cybersecurity for Industrial Control Systems (202).	Federal, SLTT	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
202 Intermediate Cybersecurity for Industrial Control Systems, Part 2	This course provides a brief review of ICS security including a comparative analysis of IT and control system architectures, security vulnerabilities, and mitigation strategies unique to the Control System domain. Accompanying this course is a sample Process Control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions. This network is also used during the course for the hands-on exercises.	Federal, SLTT	Intermediate	1	1
Analysis Pipeline	This course is designed for network flow data analysts who use or are considering using Analysis Pipeline (http://tools.netsa.cert.org/analysis-pipeline5/index.html). The course aims to help students better understand how to incorporate streaming network flow analysis into their toolkit for identifying and alerting on events of interest.	Federal, SLTT, Veterans	Intermediate	1	1
Artificial Intelligence (AI) and Machine Learning (ML) for Cyber	The AI/ML for Cyber course is designed to provide students with an overview of the foundational practices and ethical principles of Artificial Intelligence such as reducing risk and unwanted bias to create ethical, transparent, and fair artificial intelligence systems.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Cisco CCENT Self-Study Prep	This course prepares learners for the Cisco CCENT certification. Topics include installing, operating, configuring, and verifying a basic IPv4 and IPv6 network, configuring a LAN switch, configuring an IP router, and identifying basic security threats.	Federal, SLTT, Veterans	Intermediate	4	4
Cisco CCNA Security Self-Study Prep	This 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 includes protocol sniffers, analyzers, TCP/IP, desktop utilities, Cisco IOS, the Cisco VPN, a Cisco simulation program called Packet Tracer, and some web-based resources.	Federal, SLTT, Veterans	Intermediate	4	4
Cloud Computing Security	The course explores guidance from the Cloud Security Alliance (CSA), National Institute of Standards and Technology (NIST), National Security Agency (NSA), and several Cloud Service Providers (CSPs). Topics will cover cloud security risks and threats, basic operations, incident response considerations, along with application, data and infrastructure security concepts as well as demonstrations of cloud provider tools and capabilities.	Federal, SLTT, Veterans, Public	Intermediate	2	2

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Cyber Dark Arts	This course highlights 'dark' or deceptive activities employed by malicious users via the Internet as well as topics such as zero-day attacks, dark web, alternate OSs, VPN/TOR, weaponized psychology, and anonymous services.	Federal, SLTT, Veterans, Public	Intermediate	1	1
Cybersecurity within IT & ICS Domains (210W)	Understanding the basic concepts of cybersecurity will provide the necessary foundation to determine the appropriate controls to protect ICS. ICSs are dependent on IT, as contemporary IT is often troubled with cyber vulnerabilities.	Federal, SLTT	Intermediate	1	1
Demilitarized Zone (DMZ) with IDS/IPS	This course introduces the concept of a network Demilitarized Zone (DMZ) and the security benefits it can provide as well as best practices for designing and implementing a DMZ, followed with a section on IDS and IPS systems including an in-depth look at SNORT for network monitoring.	Federal, SLTT, Veterans	Intermediate	3	3

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Emerging Cyber Security Threats	This course covers a broad range of cybersecurity elements that pose threats to information security posture such as 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.	Federal, SLTT, Veterans	Intermediate	1	1
Enterprise Cybersecurity Operations	This course highlights technical knowledge and skills required for implementing secure solutions in the enterprise. A broad spectrum of disciplines is covered to aid practitioners in applying frameworks and controls to improve the security posture while supporting the business mission.	Federal, SLTT, Veterans	Intermediate	1	1
FedRAMP: A Leader's Dashboard for Compliance	In this hour-long webinar National Defense University Professor Roxanne Everetts discusses some key leadership decisions around using Federal Risk and Authorization Management Program (FedRAMP) solutions. FedRAMP is a unique government cloud - it is a combination of cloud security, cybersecurity, and risk management.	Federal, SLTT, Veterans	Intermediate	3	3

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
IMR 204 - Vulnerabilities of Internet-Accessible Systems: Defending Internet-Accessible Systems Cyber Range Training	Content includes network mapping, identifying and remediating vulnerabilities in internet-accessible systems, and resolving password spraying attacks. Participants will use tools and work with cybersecurity engineers in a host environment with a sample hygiene assessment report to investigate the network, prioritize vulnerabilities, and apply firewall rules to your network.	Federal, SLTT	Intermediate	3	4
IMR 205 - Web and Email Server Attacks	Participants will be introduced to common web and email vulnerabilities, as well as the technologies of encryption and authentication to enhance web and email security. This exercise uses a hands-on approach to facilitate realistic technical training and interaction opportunities for learners.	Federal, SLTT	Intermediate	5	6
IMR 206 - DNS Infrastructure Attacks	Working with cybersecurity engineers in a host environment with various software applications, participants will be introduced to common DNS tampering techniques, as well as the technologies of DNS sink holing to enhance security. Learners will analyze network and host-based artifacts and implement remediation for the identified vulnerabilities.	Federal, SLTT	Intermediate	5	6

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Influence of Common IT Components on ICS (210W-02)	This course covers the elements of a traditional IT network, specific issues that relate to emerging cybersecurity problems, and some of the complexity associated with trying to mitigate those problems.	Federal, SLTT	Intermediate	2	2
Insider Threat Program Manager: Implementation and Operations	This course discusses various techniques and methods to develop, implement, and operate program components. The content covered supports organizations implementing and managing insider threat detection and prevention programs based on various government mandates or guidance.	Federal, SLTT, Veterans	Intermediate	1	1
Mapping IT Defense-in-Depth Security Solutions to ICS, Part 1	This training will introduce the defense-in-depth model and cover layers 1 and 2.	Federal, SLTT	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Mapping IT Defense-in-Depth Security Solutions to ICS, Part 2	This training will continue the defense-in-depth model and cover layer 3 - Network Security.	Federal, SLTT	Intermediate	1	1
Network Security	This Network+ prep course is a self-study resource designed to help students prepare to sit for the CompTIA Network+ 10-N007 certification exam - focuses on IT infrastructure and networking concepts for junior to mid-level IT professionals in the cyber workforce and topics like network operations, security, troubleshooting and tools, and infrastructure support.	Federal, SLTT, Veterans	Intermediate	3	3
Securing Infrastructure Devices	This course covers physical security, operating system security, management traffic security, device service hardening, securing management services and device access privileges.	Federal, SLTT, Veterans	Intermediate	3	3

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Windows Operating System Security	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.	Federal, SLTT, Veterans, Public	Intermediate	2	2
Wireless Network Security	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. (9 hours)	Federal, SLTT, Veterans	Intermediate	3	3
(ISC)² ™ CISSP ® Certification Prep	This 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.	Federal, SLTT, Veterans	Advanced	1	1

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
(ISC)² ™ CISSP Concentration: ISSEP	This course focuses on applying security and systems engineering principles into business functions to help students prepare to sit for the specialized (ISSEP) certification exam.	Federal, SLTT, Veterans	Advanced	1	1
301 ICS Cybersecurity	This course provides extensive hands-on training on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber attacks. Trainees will learn about common vulnerabilities and the importance of understanding the environment they are tasked to protect. Learning the weaknesses of a system will enable trainees to implement the mitigation strategies and institute policies and programs that will provide the defense-in-depth needed to ensure a more secure ICS environment.	Federal, SLTT	Advanced	1	1
401 ICS Evaluation	This instructor-led 5-day course provides hands-on training to analyze, evaluate, and document the cybersecurity posture of an organization's Industrial Control Systems. The course uses a multi-step process, in a simulated ICS environment to teach how to analyze cybersecurity weaknesses and threats, evaluate and map findings, document potential mitigations, and provide ongoing resolutions to strengthen the cybersecurity posture.	Federal, SLTT	Advanced	2	2

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Certified Ethical Hacker (CEHv10)	This course helps prepare students to sit for the EC-Council CEHv10 certification exam. This course helps students broaden their knowledge of advanced network assessment techniques including enumeration, scanning and reconnaissance. This course is designed for the skilled professional to use the same knowledge and tools as a malicious hacker but in an ethical and lawful manner to examine an organization's network security posture.	Federal, SLTT, Veterans	Advanced	1	1
DNSSEC Training Workshop	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. Topics include DNSSEC introduction, DNSSEC mechanisms, signing a zone, delegation signer (DS) RRs, setting up a secure resolver, server operational considerations and DNSSEC conclusions.	Federal, SLTT, Veterans	Advanced	2	2
IMR 302 - Cloud Leak: Cloud Leak Cyber Range Challenge	Scenario: Participants must capture network and host-based artifacts from the attack, report the source and extent of a compromise, and provide recommendations for hardening the network against attack and better data hygiene practices.	Federal, SLTT	Advanced	7	8

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
IMR 303 - Business Email Attack: Business Email Compromise Cyber Range Challenge	Scenario: Your organization receives an announcement that a Business Email Compromise is suspected to have occurred. Participants then use tools on the host environment to investigate the intrusion and uncover evidence. Once data collection is complete, participants submit a briefing and discuss their findings.	Federal, SLTT	Advanced	4	4
IPv6 Security Essentials	This course begins with a primer of IPv6 addressing and its current deployment state, discusses ICMPv6, DHCPv6, and DNSv6, and concludes with IPv6 Transition Mechanisms, security concerns and management strategies.	Federal, SLTT, Veterans	Advanced	3	3
ISACA Certified Information Security Manager Prep (CISM)	This certification prep self-study resource helps prepare candidates to sit for the management-focused CISM exam. The course includes concepts like Information Security Governance, Information Risk Management and Compliance, Information Security Program Development and Management, and Information Security Incident Management.	Federal, SLTT, Veterans	Advanced	1	1

Professional Development Training

◄ Prev Next ►

Operate and Maintain

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Operate and Maintain	
				Specialty Areas	Work Roles
Linux Operating Systems Security	This course introduces security features and tools available in Linux as well as the considerations, advantages, and disadvantages of using those features. The class 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.	Federal, SLTT, Veterans	Advanced	2	2
Radio Frequency Identification (RFID) Security	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.	Federal, SLTT, Veterans	Advanced	2	2
Security and DNS	This course discusses name resolution principles, name resolution and security, DNS security standards, securing zone transfers with TSIG, and DNSSEC principles, implementation and resources.	Federal, SLTT, Veterans	Advanced	3	3

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern	
				Specialty Areas	Work Roles
101 Introduction to Control Systems Cybersecurity	This course introduces students to the basics of Industrial Control Systems (ICS) cybersecurity. This includes a comparative analysis of IT and ICS architectures, understanding risk in terms of consequence, security vulnerabilities within ICS environments, and effective cyber risk mitigation strategies for the Control System domain.	Federal, SLTT	Entry	2	4
Access Control	What is Access Control? Why does this matter? What is a High Value Asset (HVA)? What issue did DHS find? Guidance for protecting HVAs	Federal, SLTT	Entry	2	6
Authentication	Why does HVA authentication matter? What does it mean to you? How can you protect your organization?	Federal, SLTT	Entry	2	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern – Specialty Areas	NICE Framework Mapping: Oversee and Govern – Work Roles
CDM 141 - Introduction to the New CDM Agency Dashboard	This course is a recording of a virtual two-hour course which is the first of six webinars. This course provides participants with the essential knowledge of the ES-2 version of the CDM Agency Dashboard. It explains basic features and navigation within the environment, and includes demonstrations using the new CDM Agency Dashboard to identify and report on vulnerabilities.	Federal, SLTT, Veterans	Entry	2	6
CDM 143 - Vulnerability Management with the CDM Agency Dashboard	This course is a recording of a virtual two-hour course which is the second of six webinars covering the ES-2 version of the CDM Agency Dashboard. This course introduces participants to CDM Agency-Wide Adaptive Risk Enumeration (AWARE) and other vulnerability management topics. With the information provided, dashboard users can identify the most critical vulnerabilities and prioritize mitigation activities at their agency.	Federal, SLTT, Veterans	Entry	2	7
CDM Agency Dashboard: The CONOPS and Beyond	Learn about the Concept of Operations (CONOPS) for the Agency CDM Dashboard. Mr. Willie Crenshaw, Program Executive for CDM, National Aeronautics and Space Administration (NASA), and Mr. Mark Singer, Guidance and Planning Team Lead for Cybersecurity Governance, Federal Network Resilience Division, review the highlights of the CDM Agency Dashboard CONOPS, what features are included through CDM Release 6, and how agencies can take full advantage of Release 6 features.	Federal, SLTT	Entry	2	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern: Specialty Areas	NICE Framework Mapping: Oversee and Govern: Work Roles
Cloud Security - What Leaders Need to Know	This course features National Defense University Professor Robert Richardson who discusses important security and oversight requirements for commercial cloud solutions.	Federal, SLTT, Veterans	Entry	4	6
Creating a Computer Security Incident Response Team (CSIRT)	This course was developed for organizations and individuals who are at the beginning of their planning and implementation process for creating a computer security incident response team or an incident management capability.	Federal, SLTT, Veterans	Entry	1	1
Critical Infrastructure Protection	This course discusses 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.	Federal, SLTT, Veterans, Public	Entry	1	1

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Oversee and Govern	
				Specialty Areas	Work Roles
Cyber Essentials	This course focuses on how leaders can develop actionable items to start implementing organizational cybersecurity practices and introduces the six essential elements of building a culture of cyber readiness.	Federal, SLTT, Veterans, Public	Entry	5	5
Cybersecurity Overview for Managers	This course is designed for managers and other stakeholders involved in decision making regarding their cyber environment, but do not have a strong technical background. 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.	Federal, SLTT, Veterans	Entry	3	3
Cybersecurity Practices for Industrial Control Systems (100W)	This training will cover standard cybersecurity practices with information specific to industrial control systems (ICS). It highlights the type of information an adversary may view as valuable. The training provides tools to recognize potential weaknesses in daily operations, as well as effective techniques to address those weaknesses.	Federal, SLTT	Entry	1	2

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Oversee and Govern	
				Specialty Areas	Work Roles
Don't Wake Up to a Ransomware Attack	This course provides essential knowledge and reviews real-life examples of these attacks to help you and your organization to prevent, mitigate, and respond to the ever-evolving threat of ransomware.	Federal, SLTT, Veterans	Entry	4	9
Elections and IT - Embrace your role as a Manager	The course serves as an overview of information technology and how to ensure security is included in the planning, procuring, designing, implementing, and maintaining of interconnected electronic election systems, including public-facing websites. The content introduces the key concepts of identifying vulnerabilities and how to protect election systems from internal and external threats and provides information on cybersecurity resources available from the EAC and DHS.	Federal, SLTT, Veterans	Entry	1	1
Enterprise Risk Management	What is ERM? What is a High Value Asset? Why does ERM matter to HVAs? What does ERM mean to HVAs? How should Federal agencies plan to address this finding?	Federal, SLTT	Entry	2	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern	
				Specialty Areas	Work Roles
Foundations of Cybersecurity for Managers	This course is designed for managers and other stakeholders who may be involved in decision making that would include considerations for security in a cyber environment but do not have a strong technical background. The course aims to help the learner better understand how people and technology work together to protect mission critical assets, and the frameworks leveraged to assess and apply security controls.	Federal, SLTT, Veterans	Entry	2	2
Fundamentals of Cyber Risk Management	Fundamentals of Cyber Risk Management covers key concepts, issues, and considerations for managing risk. Discussions include identifying critical assets and operations, risk assessment and analysis methodologies, risk management frameworks, and how to determine threats to your business function, mitigation strategies, and response and recovery.	Federal, SLTT, Veterans	Entry	1	1
How Data Consistency Impacts CDM	Learn more about how data consistency impacts CDM from Mr. Rick McMaster, CDM Program Management Office. This webinar includes open discussions with attendees to better understand challenges and lessons learned.	Federal, SLTT	Entry	2	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern	
				Specialty Areas	Work Roles
How Identity, Credential, and Access Management (ICAM) Protects Your Agencies' Assets	Learn about the importance of ICAM in the context of the CDM Program and the "life cycle" of agencies' employees as they join, move in, then leave an organization. A one-hour webinar on ICAM -the credential management issues that arise during CDM Phase 2, how ICAM factors into cloud computing, and the zero-trust approach to access control.	Federal, SLTT	Entry	2	6
How to Address the Threat of Ransomware Attacks	What is Ransomware? How does it work? What are the signs of infection? What can you do?	Federal, SLTT	Entry	2	6
ICS Cybersecurity Landscape for Managers (FRE2115 R00)	The purpose of this course is to provide the necessary background and basic understanding of the current Industrial Control System (ICS) cybersecurity landscape for decision makers working in an ICS environment. It includes an overview of the elements of the risk equation and how it applies to the cybersecurity of an ICS. Trainees will be introduced to actual threats, vulnerabilities, and consequences, along with tools they can use to help mitigate the cybersecurity risk to their ICS.	Federal, SLTT	Entry	2	3

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern: Specialty Areas	NICE Framework Mapping: Oversee and Govern: Work Roles
IMR 001 - Ransomware	This course includes an overview of ransomware attacks and how threat actors compromise systems to lock out legitimate users and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	4	6
IMR 002 - Cloud Security	This course includes an overview of cloud-based environment attacks and how threat actors compromise systems to damage operations, escalate privileges, and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	4	6
IMR 003 - Business Email Compromise	This course puts you front and center for a live, two-hour red team/ blue team cyber range demonstration of a Business Email Compromise cyberattack. Be in the room where it happens, guided by expert engineers through the attack and defense strategy of each side to impart understanding and essential takeaways that prepare you and your organization for what it takes to orchestrate an effective response to a real-time cyberattack.	Federal, SLTT	Entry	4	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern – Specialty Areas	NICE Framework Mapping: Oversee and Govern – Work Roles
IMR 102 - Cloud-based server attacks: Don't Get Caught in the Storm	An overview of cloud computing and its associated security vulnerabilities, common signs of a cloud server attack and how to respond to suspicious activity, CISA guidance and best practices to mitigate cloud server vulnerabilities, secure cloud systems, and block threat activity, case studies demonstrating the impacts of cloud attacks, including major data breaches.	Federal, SLTT	Entry	5	11
IMR 103 - Business Email Compromise: Preventing Business Email Attacks	An overview of business email compromise, phishing, and its impact on organizations. Learn how to identify a business email attack, mitigate the likelihood and impact of BEC through best practices, and respond and recover funds in the event of an attack.	Federal, SLTT	Entry	4	6
IMR 104 - Internet-Accessible System Vulnerabilities: Don't Let Cyber Criminals Steal Your Connections	Internet-accessible systems have become the backbone of modern business and communication infrastructure, from smartphones to web applications such as Outlook to the explosive growth of the "Internet of Things" (IoT). Each of these systems and devices, however, can be targeted by threat actors and used to conduct malicious activity if they are unsecured.	Federal, SLTT	Entry	4	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern	
				Specialty Areas	Work Roles
IMR 105 - Web and Email Server Attacks: Securing Web and Email Servers	Web and email servers are the workhorses of the Internet: we couldn't run government, businesses, or our personal lives without them! However, the information exchanged through web and email servers can offer a tempting target for cyber attackers. Key Guidance for Organizations: CISA provides resources and best practices to help individuals and organizations secure their web and email infrastructure.	Federal, SLTT	Entry	3	4
IMR 106 - DNS Infrastructure Tampering: Strengthen Your Resolve	Understand DNS and its vulnerabilities: Learn how the Domain Name System works, and how threat actors target its vulnerabilities to conduct malicious activity. Identify signs of a DNS attack: Understand common red flags that indicate potential attack, and how to verify suspicious activity. Receive CISA guidance and best practices: Review official CISA guidance to help organizations prevent, mitigate, and recover from DNS attacks.	Federal, SLTT	Entry	3	9
IMR 107 - High-Value Assets	Define high value assets, and how to assess and prioritize risks. Understand the most likely threats to HVAs and how to mitigate associated vulnerabilities. Learn the steps and parameters to identify, categorize, prioritize, and secure your HVAs or critical assets. Explore the impacts of documented critical or high value asset cyberattacks, and the success of resulting response and recovery efforts.	Federal, SLTT	Entry	4	10

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Oversee and Govern	
				Specialty Areas	Work Roles
Incident Response 101	This course reviews malware types and vectors for compromise, common issues hindering an effective response, best practices for preparing and responding to an infection incident, and defensive measures to strengthen the cybersecurity posture.	Federal, SLTT, Veterans	Entry	1	1
ISCM E-Learning Module	This course provide introductory information on the importance of building an ISCM strategy, how ISCM integrates with an organization's Enterprise Risk Management (ERM) strategy, and ISCM program management and execution	Federal, SLTT	Entry	2	6
Learn How CDM's AWARE Scoring Can Help You Reduce Cyber Risk	Learn how AWARE works, and how it can be used to reduce risks across the federal enterprise - an overview of the scoring methodology behind AWARE, and what you need to do to improve your agency's score. Insights on how AWARE could evolve as agencies gain more experience with CDM to support information security continuous monitoring policies.	Federal, SLTT	Entry	2	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern – Specialty Areas	NICE Framework Mapping: Oversee and Govern – Work Roles
LEGACY CDM Agency Dashboard Asset Discovery Bootcamp (CDM110)	This course incorporates the first three CDM Agency Dashboard training courses into one two-day event and allows additional time for hands-on exercises and questions. The class includes all content from: Introduction to Creating Queries & Reports; Using Measurement & Metrics of Hardware & Software Assets; Using the CDM Agency Dashboard to Drive Your Vulnerability Management Work Plan.	Federal, SLTT, Veterans	Entry	2	6
LEGACY Introduction to Creating Queries & Reports Using the CDM Agency Dashboard (CDM102)	This course provides participants with the basic knowledge of continuous monitoring concepts. It includes four live demonstrations using the search, query, and reporting capabilities of the CDM Agency Dashboard to identify and report on vulnerabilities.	Federal, SLTT, Veterans	Entry	2	6
LEGACY Using Measurements & Metrics of Hardware & Software Assets with the CDM Agency Dashboard (CDM103)	This course presents an overview of how the dashboard provides visibility into the metrics and measurements needed for a continuous monitoring program; explains how to create queries for HW and SW assets; and introduces a framework for using data reports to inform risk-based decision-making.	Federal, SLTT, Veterans	Entry	2	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern: Specialty Areas	NICE Framework Mapping: Oversee and Govern: Work Roles
LEGACY Using the CDM Agency Dashboard to Drive Your Vulnerability Management Work Plan	This course introduces participants to CDM Agency-Wide Adaptive Risk Enumeration (AWARE).	Federal, SLTT, Veterans	Entry	2	6
Let's Talk About Aware...	In this 17-minute episode, David Otto, a Risk Management Subject Matter Expert with the Continuous Diagnostics & Mitigation Program, talks about how agencies can optimize the use of Agency-Wide Adaptive Risk Enumeration (AWARE) – an algorithm tied into the CDM Federal Dashboard that helps agencies measure risk. Other topics include how agencies can interpret and socialize their AWARE results and how AWARE and the Risk Management Framework complement each other to mitigate risk.	Federal, SLTT	Entry	2	6
Malware Defense	This course presents an overview of how the dashboard provides visibility into the metrics and measurements needed for a continuous monitoring program; explains how to create queries for HW and SW assets; and introduces a framework for using data reports to inform risk-based decision-making.	Federal, SLTT	Entry	2	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Oversee and Govern	
				Specialty Areas	Work Roles
Measuring What Matters: Security Metrics Workshop	This workshop focuses on how to measure the right things in order to make informed management decisions, take the appropriate actions, and change behaviors. Students will learn how to refine a strategic or business objective that meets that S.M.A.R.T.E.R. criteria: Specific, Measurable, Achievable, Relevant, Time-bound, Evaluated, Reviewed, and can be used to initiate the Goal - Question - Indicator - Metric (GQIM) process.	Federal, SLTT, Veterans	Entry	1	1
Mobile and Device Security	This 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. (22 Hours)	Federal, SLTT, Veterans	Entry	1	1
New CDM Agency Dashboard Videos (8 Videos)	These short videos (5-11 minutes) of the new CDM Agency Dashboard provide a foundation level of knowledge and background that will help end users of the dashboard prepare for training demonstrations and hands-on activities, as well as the implementation of the new dashboard.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Oversee and Govern	
				Specialty Areas	Work Roles
Patch Management	What is a High Value Asset? Why is this Patch Management finding important? What types of challenges do organizations face with Patch Management? What steps should your organization take to respond to this finding?	Federal, SLTT	Entry	2	6
Ransomware	How to Address the Threat of Ransomware Attacks. What is Ransomware? How it works? What are the signs of infection? What can you do?	Federal, SLTT	Entry	2	6
Risk Management Framework for Leaders	This webinar recorded on July 10, 2020 features National Defense University Professor Mark Duke discussing key leadership decisions to implement the NIST Risk Management Framework (RMF). The RMF is a risk-based approach to implement security within an existing enterprise - it is leadership's responsibility to ensure adequate and effective system security.	Federal, SLTT, Veterans	Entry	5	11

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern	
				Specialty Areas	Work Roles
Securing Internet-Accessible Systems	This course focuses on Internet-accessible systems or "Internet of Things" (IoT). Each of these systems and devices can be targeted by threat actors and used to conduct malicious activity if they are unsecured, or worse, these systems can leave vulnerabilities and sensitive information open to exploitation if not properly configured and maintained. This course explains the vulnerabilities of internet-accessible systems and how to prepare for, mitigate, and respond to a potential attack.	Federal, SLTT, Veterans	Entry	3	9
Static Code Analysis Using HPE Fortify	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 Fortify is used to identify and remove Common Weakness Enumeration (CWE) from applications in which the source code is available.	Federal, SLTT, Veterans	Entry	1	1
Static Code Analysis Using Synopsis Coverity	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. (1.5 Hours)	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern	
				Specialty Areas	Work Roles
Supply Chain Assurance Using Sonatype Nexus	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 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.	Federal, SLTT, Veterans	Entry	1	1
The Election Official as IT Manager	This course focuses on why Election Officials must view themselves as IT systems managers and introduces the knowledge and skills necessary to effectively function as an IT manager. The content also covers Social Media and Website best practices, vulnerabilities, and liabilities, and addresses Procuring IT, Vendor Selection, Testing and Audits, Security Measures, and Risk Assessments.	Federal, SLTT, Veterans	Entry	1	1
Understanding DNS Attacks	This course provides key information you need to know to protect yourself and your organization from DNS infrastructure tampering including common vulnerabilities, how to identify a potential attack, and guidance and best practices to mitigate the likelihood and impact of a successful DNS attack.	Federal, SLTT, Veterans	Entry	4	10

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern – Specialty Areas	NICE Framework Mapping: Oversee and Govern – Work Roles
Understanding Web and Email Server Security	Understanding Web and Email Server Security	Federal, SLTT, Veterans	Entry	3	9
Using the CDM Agency Dashboard to Combat WannaCry Ransomware	This 15-minute video explains how a Federal Agency can use the CDM Agency dashboard to identify and mitigate system vulnerabilities that are exploited by the WannaCry Ransomware malware. The video demonstrates tasks that can be carried out in the CDM Agency dashboard to manage risks to agency systems and information that might be otherwise taken advantage of by this negative threat	Federal, SLTT	Entry	2	6
Vulnerability Management Using Drupal	The 10-minute video describes how the CDM program can be used to identify and remediate cybersecurity risks through vulnerability management using the example of Drupal Security Alerts.	Federal, SLTT	Entry	2	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern	
				Specialty Areas	Work Roles
(ISC)² ™ CAP (R) Prep Self Study	This certification prep course helps prepare students strengthen their knowledge and skills in understanding security and authorization of information, categorizing information systems, selecting security controls, implementing security controls, assessing security controls, authorizing information systems and monitoring security controls.	Federal, SLTT, Veterans	Intermediate	1	1
201 Intermediate Cybersecurity for Industrial Control Systems, Part 1	This course provides technical instruction on the protection of Industrial Control Systems using offensive and defensive methods. Attendees will recognize how cyber attacks are launched, why they work, and mitigation strategies to increase the cybersecurity posture of their Control System networks. This course acts as a prerequisite for the next course, Intermediate Cybersecurity for Industrial Control Systems (202).	Federal, SLTT	Intermediate	1	2
202 Intermediate Cybersecurity for Industrial Control Systems, Part 2	This course provides a brief review of Industrial Control Systems security, including a comparative analysis of IT and control system architectures, security vulnerabilities, and mitigation strategies unique to the Control System domain. Because this course is hands-on, students will get a deeper understanding of how the various tools work.	Federal, SLTT	Intermediate	1	2

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Oversee and Govern	
				Specialty Areas	Work Roles
Attack Methodologies in IT & ICS (210W-09)	Understanding how hackers attack systems helps you better understand how to defend against cyber attacks.	Federal, SLTT	Intermediate	1	2
Common ICS Components (210W-03)	This course covers the common components found in Industrial Control Systems (ICS). It reviews the components found in most ICS.	Federal, SLTT	Intermediate	1	2
Current Trends (Threat) (210W-06)	Risk is a function of threat, vulnerability, and consequence. The most complex attribute is threat because it can be intentional or unintentional, natural or man-made. When trying to develop defensive strategies to protect controls systems, it is important to understand the threat landscape in order for appropriate countermeasures or compensating controls to be deployed.	Federal, SLTT	Intermediate	2	2

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern – Specialty Areas	NICE Framework Mapping: Oversee and Govern – Work Roles
Current Trends (Vulnerabilities) (210W-07)	In this course, we examine some of the current trends in cybersecurity vulnerabilities that contribute directly to cyber risk in Industrial Control Systems (ICSs). The goal is to identify the root causes and their associated countermeasures that can be used to protect control systems.	Federal, SLTT	Intermediate	2	2
Cyber Supply Chain Risk Management	This course focuses on cyber supply chain risk management, also known as C-SCRM, and the role it plays within our society today. This course will explain how to securely provision, analyze, oversee and govern, protect and defend a supply chain.	Federal, SLTT, Veterans, Public	Intermediate	3	3
Cybersecurity Risk (210W-05)	This course is designed to help you gain a better understanding of cyber risk, how it is defined in the context of ICS security, and the factors that contribute to risk. This will empower you to develop cybersecurity strategies that align directly with the ICS environment. Also, learn how IT-based countermeasures can be customized to accommodate for the uniqueness of ICS architectures.	Federal, SLTT	Intermediate	2	2

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern – Specialty Areas	NICE Framework Mapping: Oversee and Govern – Work Roles
Cybersecurity within IT & ICS Domains (210W)	Understanding the basic concepts of cybersecurity will provide the necessary foundation to determine the appropriate controls to protect ICS. ICSs are dependent on IT, as contemporary IT is often troubled with cyber vulnerabilities.	Federal, SLTT	Intermediate	1	2
Differences in Deployments of Industrial Control Systems (210W-01)	This course discusses what, where, and how industrial control systems (ICSs) are used and describes some of specific examples of how ICSs work in real-life situations.	Federal, SLTT	Intermediate	1	2
Emerging Cyber Security Threats	This course covers a broad range of cybersecurity elements that pose threats to information security posture such as 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.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern – Specialty Areas	NICE Framework Mapping: Oversee and Govern – Work Roles
FedRAMP: A Leader's Dashboard for Compliance	In this hour-long webinar National Defense University Professor Roxanne Everetts discusses some key leadership decisions around using Federal Risk and Authorization Management Program (FedRAMP) solutions. FedRAMP is a unique government cloud - it is a combination of cloud security, cybersecurity, and risk management.	Federal, SLTT, Veterans	Intermediate	5	11
ICS Cybersecurity Consequences (210W-08)	A cyber attack that results in the release of a toxic chemical and kills 10 people is more significant than a cyber attack that temporarily disables the HVAC in a control – or is it? This course will help you understand the impacts of cyber attack can have on an ICS & provide you with different ways of looking at the potential consequences of three types of events.	Federal, SLTT	Intermediate	1	2
IMR 204 - Vulnerabilities of Internet-Accessible Systems: Defending Internet-Accessible Systems Cyber Range Training	Four activities that explore the following aspects: network mapping, identifying and remediating vulnerabilities in internet-accessible systems, and resolving password spraying attacks. Participants will use tools and work with cybersecurity engineers in a host environment with a sample hygiene assessment report to investigate the network, prioritize vulnerabilities, and apply firewall rules to your network.	Federal, SLTT	Intermediate	4	9

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern – Specialty Areas	NICE Framework Mapping: Oversee and Govern – Work Roles
IMR 205 - Web and Email Server Attacks	Participants will be introduced to common web and email vulnerabilities, as well as the technologies of encryption and authentication to enhance web and email security. This exercise uses a hands-on approach to facilitate realistic technical training and interaction opportunities for learners.	Federal, SLTT	Intermediate	3	9
IMR 206 - DNS Infrastructure Attacks	Working with cybersecurity engineers in a host environment with various software applications, participants will be introduced to common DNS tampering techniques, as well as the technologies of DNS sinkholing to enhance security. Learners will analyze network and host-based artifacts and implement remediation for the identified vulnerabilities.	Federal, SLTT	Intermediate	4	6
Influence of Common IT Components on ICS (210W-02)	This course covers the elements of a traditional IT network, specific issues that relate to emerging cybersecurity problems, and some of the complexity associated with trying to mitigate those problems.	Federal, SLTT	Intermediate	1	2

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Oversee and Govern	
				Specialty Areas	Work Roles
Managing Computer Security Incident Response Teams (CSIRTS)	This course provides an overview of the incident response field, including the nature of incident response activities and incident handling processes, as well as foundational material, staffing issues, incident management processes and other issues such as working with law enforcement, insider threat and publishing information.	Federal, SLTT, Veterans	Intermediate	2	2
Mapping IT Defense-in-Depth Security Solutions to ICS, Part 1	This training will introduce the defense-in-depth model and cover layers 1 and 2.	Federal, SLTT	Intermediate	1	2
Mapping IT Defense-in-Depth Security Solutions to ICS, Part 2	This training will continue the defense-in-depth model and cover layer 3 - Network Security.	Federal, SLTT	Intermediate	1	2

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Oversee and Govern	
				Specialty Areas	Work Roles
SiLK Traffic Analysis	This course is designed to teach the analyst how to make network flow analysis a part of their workflow. Students will learn how to use the SiLK network flow analysis tool suite to perform tasks such as querying for records related to a specific incident or indicator, creating sets of indicators for batch analysis, and leveraging network flow to provide basic network situational awareness.	Federal, SLTT, Veterans	Intermediate	1	1
Software Assurance Executive (SAE) Course	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. (10 hours	Federal, SLTT, Veterans	Intermediate	2	2
(ISC)² ™ CISSP (R) Certification Prep	This 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.	Federal, SLTT, Veterans	Advanced	1	1

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Oversee and Govern	
				Specialty Areas	Work Roles
(ISC)2 ™ CISSP Concentration: ISSEP	This course focuses on applying security and systems engineering principles into business functions to help students prepare to sit for the specialized (ISSEP) certification exam.	Federal, SLTT, Veterans	Advanced	1	1
(ISC)2 ™ CISSP Concentration: ISSMP Prep	This course focuses on applying security and systems engineering principles into business functions to help students prepare to sit for the specialized (ISSEP) certification exam.	Federal, SLTT, Veterans	Advanced	2	2
301 ICS Cybersecurity	This course provides extensive hands-on training on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber attacks. Trainees will learn about common vulnerabilities and the importance of understanding the environment they are tasked to protect. Learning the weaknesses of a system will enable trainees to implement the mitigation strategies and institute policies and programs that will provide the defense-in-depth needed to ensure a more secure ICS environment.	Federal, SLTT	Advanced	1	2

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Oversee and Govern – Specialty Areas	NICE Framework Mapping: Oversee and Govern – Work Roles
401 ICS Evaluation	This 5-day course provides hands-on training on how to analyze, evaluate, and document the cybersecurity posture of an organization's Industrial Control Systems (ICS) for the purpose of identifying recommended changes. Specifically, the course will utilize a multi-step repeatable process, within a simulated ICS environment, that teaches how to analyze cybersecurity weaknesses and threats, evaluate and map findings, document potential mitigations, and provide ongoing resolutions to strengthen the cybersecurity posture.	Federal, SLTT	Intermediate	2	2
IMR 302 - Cloud Leak: Cloud Leak Cyber Range Challenge	Scenario: Participants must capture network and host-based artifacts from the attack, report the source and extent of a compromise, and provide recommendations for hardening the network against attack and better data hygiene practices.	Federal, SLTT	Intermediate	5	11
IMR 303 - Business Email Attack: Business Email Compromise Cyber Range Challenge	Scenario: Your organization receives an announcement that a Business Email Compromise is suspected to have occurred. Participants then use tools on the host environment to investigate the intrusion and uncover evidence. Once data collection is complete, participants submit a briefing and discuss their findings.	Federal, SLTT	Intermediate	4	6

Professional Development Training

◄ Prev Next ►

Oversee and Govern

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Oversee and Govern	
				Specialty Areas	Work Roles
ISACA Certified Information Security Manager Prep (CISM)	This certification prep self-study resource helps prepare candidates to sit for the management-focused CISM exam. The course includes concepts like Information Security Governance, Information Risk Management and Compliance, Information Security Program Development and Management, and Information Security Incident Management.	Federal, SLTT, Veterans	Advanced	2	2

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
101 Introduction to Control Systems Cybersecurity	This course introduces students to the basics of Industrial Control Systems (ICS) cybersecurity. This includes a comparative analysis of IT and ICS architectures, understanding risk in terms of consequence, security vulnerabilities within ICS environments, and effective cyber risk mitigation strategies for the Control System domain.	Federal, SLTT	Entry	1	1
CDM 143 - Vulnerability Management with the CDM Agency Dashboard	This course is a recording of a virtual two-hour course which is the second of six webinars covering the ES-2 version of the CDM Agency Dashboard. This course introduces participants to CDM Agency-Wide Adaptive Risk Enumeration (AWARE) and other vulnerability management topics. With the information provided, dashboard users can identify the most critical vulnerabilities and prioritize mitigation activities at their agency.	Federal, SLTT, Veterans	Entry	1	1
CMaaS Classroom Sessions	This course is part of the CMaaS transitional webinar series conducted via WebEx. Each video focuses on a single tool within the CMaaS solution stack and includes two major Use Cases for each tool.	Federal, SLTT, Veterans	Entry	4	4

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
CMaaS Overview	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). This course explains how Continuous Monitoring as a Service (CMaaS) relates to the Continuous Diagnostics and Mitigation (CDM) program.	Federal, SLTT, Veterans	Entry	4	4
CMaaS Technical Overview	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 learner better understand how Continuous Monitoring as a Service (CMaaS) will be implemented in DHS Component networks.	Federal, SLTT, Veterans	Entry	4	4
Critical Infrastructure Protection	This course discusses 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.	Federal, SLTT, Veterans, Public	Entry	2	2

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Cyber Security Investigations	This course discusses the basic concepts of cybersecurity and digital forensics investigation practices such as performing collection and triage of digital evidence in response to an incident, evidence collection methodologies, and forensic best practices.	Federal, SLTT, Veterans	Entry	1	1
Cybersecurity for Technical Staff	This course highlights topics such as risk management, architecture and design, and tools and technologies as well as key concepts for detecting, protecting, and defending from security threats.	Federal, SLTT, Veterans	Entry	2	2
Cybersecurity Practices for Industrial Control Systems (100W)	This training will cover standard cybersecurity practices with information specific to industrial control systems (ICS). It highlights the type of information an adversary may view as valuable. The training provides tools to recognize potential weaknesses in daily operations, as well as effective techniques to address those weaknesses.	Federal, SLTT	Entry	1	1

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Don't Wake Up to a Ransomware Attack	This course provides essential knowledge and reviews real-life examples of these attacks to help you and your organization to prevent, mitigate, and respond to the ever-evolving threat of ransomware.	Federal, SLTT, Veterans	Entry	4	4
Elections and IT - Embrace your role as a Manager	The course serves as an overview of information technology and how to ensure security is included in the planning, procuring, designing, implementing, and maintaining of interconnected electronic election systems, including public-facing websites. The content introduces the key concepts of identifying vulnerabilities and how to protect election systems from internal and external threats and provides information on cybersecurity resources available from the EAC and DHS.	Federal, SLTT, Veterans	Entry	1	1
Foundations of Incident Management	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.	Federal, SLTT, Veterans	Entry	2	2

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Fundamentals of Cyber Risk Management	This course covers key concepts, issues, and considerations for managing risk. Discussions include identifying critical assets and operations, risk assessment and analysis methodologies, risk management frameworks, and how to determine threats to your business function, mitigation strategies, and response and recovery.	Federal, SLTT, Veterans	Entry	1	1
Hacker 101 and Secure Coding	This course is designed to introduce students to the basic concepts of hacker activity, understand how to combat such activities, and learn how to reduce the risk of cyber-attacks by understanding the hacker mindset. The course covers reconnaissance before a hacker attack, exploiting a system and performing an attack, and post-exploit activities.	Federal, SLTT, Veterans, Public	Entry	1	1
IMR 001 - Ransomware	The course includes an overview of ransomware attacks and how threat actors compromise systems to lock out legitimate users and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	4	4

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
IMR 002 - Cloud Security	The course includes an overview of cloud-based environment attacks and how threat actors compromise systems to damage operations, escalate privileges, and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	4	4
IMR 003 - Business Email Compromise	This course puts you front and center for a live, two-hour red team/ blue team cyber range demonstration of a Business Email Compromise cyberattack. Be in the room where it happens, guided by expert engineers through the attack and defense strategy of each side to impart understanding and essential takeaways that prepare you and your organization for what it takes to orchestrate an effective response to a real-time cyberattack.	Federal, SLTT	Entry	2	2
IMR 102 - Cloud-based server attacks: Don't Get Caught in the Storm	An overview of cloud computing and its associated security vulnerabilities, common signs of a cloud server attack and how to respond to suspicious activity, CISA guidance and best practices to mitigate cloud server vulnerabilities, secure cloud systems, and block threat activity, case studies demonstrating the impacts of cloud attacks, including major data breaches	Federal, SLTT	Entry	4	4

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
IMR 103 - Business Email Compromise: Preventing Business Email Attacks	An overview of business email compromise, phishing, and its impact on organizations. Learn how to identify a business email attack, mitigate the likelihood and impact of BEC through best practices, and respond and recover funds in the event of an attack.	Federal, SLTT	Entry	2	2
IMR 104 - Internet-Accessible System Vulnerabilities: Don't Let Cyber Criminals Steal Your Connections	Internet-accessible systems have become the backbone of modern business and communication infrastructure, from smartphones to web applications such as Outlook to the explosive growth of the "Internet of Things" (IoT). Each of these systems and devices, however, can be targeted by threat actors and used to conduct malicious activity if they are unsecured.	Federal, SLTT	Entry	2	2
IMR 105 - Web and Email Server Attacks: Securing Web and Email Servers	Web and email servers are the workhorses of the Internet: we couldn't run government, businesses, or our personal lives without them! However, the information exchanged through web and email servers can offer a tempting target for cyber attackers. Key Guidance for Organizations: CISA provides resources and best practices to help individuals and organizations secure their web and email infrastructure.	Federal, SLTT	Entry	3	3

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
IMR 106 - DNS Infrastructure Tampering: Strengthen Your Resolve	Understand DNS and its vulnerabilities: Learn how the Domain Name System works, and how threat actors target its vulnerabilities to conduct malicious activity. Identify signs of a DNS attack: Understand common red flags that indicate potential attack, and how to verify suspicious activity. Receive CISA guidance and best practices: Review official CISA guidance to help organizations prevent, mitigate, and recover from DNS attacks.	Federal, SLTT	Entry	3	5
IMR 107 - High-Value Assets	Define high value assets, and how to assess and prioritize risks. Understand the most likely threats to HVAs and how to mitigate associated vulnerabilities. Learn the steps and parameters to identify, categorize, prioritize, and secure your HVAs or critical assets. Explore the impacts of documented critical or high value asset cyberattacks, and the success of resulting response and recovery efforts.	Federal, SLTT	Entry	4	6
Incident Response 101	This course reviews malware types and vectors for compromise, common issues hindering an effective response, best practices for preparing and responding to an infection incident, and defensive measures to strengthen the cybersecurity posture.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Introduction to Threat Hunting Teams	This course provides basic definitions, activities, and examples of teams hunting threats in the cyber domain. Content covers how hunting teams establish goals, methods used by threat hunting teams, and sources available to help read and interpret the threat landscape.	Federal, SLTT, Veterans	Entry	2	2
LAN Security Using Switch Features	Students will learn different methods of how to secure Local Area Networks (LANs) at the connectivity level. Topics include monitoring MAC addresses and port security, limiting MAC & IP spoofing, controlling traffic flows, implementing and enhancing security in VLANs, enabling authentication on connection points, and determining host security health.	Federal, SLTT, Veterans	Entry	2	2
Offensive and Defensive Network Operations	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.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Overview of Creating and Managing Computer Security Incident Response Teams (CSIRTs)	This course is designed to provide the learner with an overview of what is needed to create and operate a CSIRT. The intended audience is individuals tasked with creating a CSIRT and those who may be new to CSIRT issues and processes. Topics covered within the course include the benefits and limitations of a CSIRT, CSIRT requirements, services, common policies and procedures, and operational best practices.	Federal, SLTT, Veterans	Entry	2	2
Securing Internet-Accessible Systems	This course focuses on Internet-accessible systems or "Internet of Things" (IoT). It explains the vulnerabilities of internet-accessible systems and how to prepare for, mitigate, and respond to a potential attack. This course provides key knowledge to inform organizational awareness of internet-accessible system attacks, best practices that minimize the success of an attack, and enable effective response and recovery if an attack occurs.	Federal, SLTT, Veterans	Entry	3	3
The Election Official as IT Manager	This course focuses on why Election Officials must view themselves as IT systems managers and introduces the knowledge and skills necessary to effectively function as an IT manager. It includes a review of Election Systems, Election Night Reporting, and Interconnected Election Systems vulnerabilities and liabilities. The content also covers Social Media and Website best practices, vulnerabilities, and liabilities, and addresses Procuring IT, Vendor Selection, Testing and Audits, Security Measures, and Risk Assessments.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Understanding DNS Attacks	This course provides key information you need to know to protect yourself and your organization from DNS infrastructure tampering including common vulnerabilities, how to identify a potential attack, and guidance and best practices to mitigate the likelihood and impact of a successful DNS attack.	Federal, SLTT, Veterans	Entry	3	3
Understanding Web and Email Server Security	Understanding Web and Email Server Security	Federal, SLTT, Veterans	Entry	4	4
(ISC)² ™ CAP (R) Prep Self Study	This certification prep course helps prepare students strengthen their knowledge and skills in understanding security and authorization of information, categorizing information systems, selecting security controls, implementing security controls, assessing security controls, authorizing information systems and monitoring security controls.	Federal, SLTT, Veterans	Intermediate	2	2

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
201 Intermediate Cybersecurity for Industrial Control Systems, Part 1	This course provides technical instruction on the protection of Industrial Control Systems using offensive and defensive methods. Attendees will recognize how cyber attacks are launched, why they work, and mitigation strategies to increase the cybersecurity posture of their Control System networks. This course acts as a prerequisite for the next course, Intermediate Cybersecurity for Industrial Control Systems (202).	Federal, SLTT	Intermediate	2	2
202 Intermediate Cybersecurity for Industrial Control Systems, Part 2	This course provides a brief review of Industrial Control Systems security. It includes a comparative analysis of IT and control system architectures, security vulnerabilities, and mitigation strategies unique to the Control System domain. The hands-on nature will give students a deeper understanding of how the various tools work. Accompanying this course is a sample Process Control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions. This network is also used during the course for the hands-on exercises that will help the students develop Control Systems cybersecurity skills they can apply in their work environment.	Federal, SLTT	Intermediate	2	2
Advanced PCAP Analysis and Signature Development (APA)	This course takes users through an introduction to rules, goes over example syntax, protocols and expressions. This course contains several supporting video demonstrations as well as lab exercises writing and testing basic rules.	Federal, SLTT, Veterans	Intermediate	2	2

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Analysis Pipeline	This course is designed for network flow data analysts who use or are considering using Analysis Pipeline (http://tools.netsa.cert.org/analysis-pipeline5/index.html) as well as cybersecurity researchers. It aims to help students 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.	Federal, SLTT, Veterans	Intermediate	1	1
Attack Methodologies in IT & ICS (210W-09)	Understanding how hackers attack systems helps you better understand how to defend against cyber attacks.	Federal, SLTT	Intermediate	2	2
Current Trends (Threat) (210W-06)	Risk is a function of threat, vulnerability, and consequence. The most complex attribute is threat because it can be intentional or unintentional, natural or man-made. When trying to develop defensive strategies to protect controls systems, it is important to understand the threat landscape in order for appropriate countermeasures or compensating controls to be deployed.	Federal, SLTT	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Protect and Defend	
				Specialty Areas	Work Roles
Current Trends (Vulnerabilities) (210W-07)	In this course, we examine some of the current trends in cybersecurity vulnerabilities that contribute directly to cyber risk in Industrial Control Systems (ICSs). The goal is to identify the root causes and their associated countermeasures that can be used to protect control systems.	Federal, SLTT	Intermediate	1	1
Cyber Dark Arts	This course highlights 'dark' or deceptive activities employed by malicious users via the Internet as well as topics such as zero-day attacks, dark web, alternate OSs, VPN/TOR, weaponized psychology, and anonymous services.	Federal, SLTT, Veterans, Public	Intermediate	1	1
Cyber Supply Chain Risk Management	This course focuses on cyber supply chain risk management, also known as C-SCRM, and the role it plays within our society today. This course will explain how to securely provision, analyze, oversee and govern, protect and defend a supply chain.	Federal, SLTT, Veterans, Public	Intermediate	2	2

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Cybersecurity Analyst	The Cybersecurity Analyst course is designed to help reinforce concepts that require monitoring and information analysis to respond to suspicious events. This intermediate-level course focuses on defense techniques leveraging data and tools to identify risks to an organization, and apply effective mitigation strategies to detect and respond to threats.	Federal, SLTT, Veterans	Intermediate	3	3
Cybersecurity within IT & ICS Domains (210W)	Understanding the basic concepts of cybersecurity will provide the necessary foundation to determine the appropriate controls to protect ICS. ICSs are dependent on IT, as contemporary IT is often troubled with cyber vulnerabilities.	Federal, SLTT	Intermediate	2	2
Demilitarized Zone (DMZ) with IDS/IPS	This course introduces the concept of a network Demilitarized Zone (DMZ) and the security benefits it can provide as well as best practices for designing and implementing a DMZ, followed with a section on IDS and IPS systems including an in-depth look at SNORT for network monitoring. The course concludes with log analysis and management best practices.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Emerging Cyber Security Threats	This course covers a broad range of cybersecurity elements that pose threats to information security posture such as 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.	Federal, SLTT, Veterans	Intermediate	1	1
ICS Cybersecurity Consequences (210W-08)	A cyber attack that results in the release of a toxic chemical and kills 10 people is more significant than a cyber attack that temporarily disables the HVAC in a control – or is it? This course will help you better understand the impacts of cyber based attack can have on an ICS and provide you with different ways of looking at the potential consequences of three types of events.	Federal, SLTT	Intermediate	1	1
IMR 204 - Vulnerabilities of Internet-Accessible Systems: Defending Internet-Accessible Systems Cyber Range Training	Four activities that explore the following aspects: network mapping, identifying and remediating vulnerabilities in internet-accessible systems, and resolving password spraying attacks. Participants will use tools and work with cybersecurity engineers in a host environment with a sample hygiene assessment report to investigate the network, prioritize vulnerabilities, and apply firewall rules to your network.	Federal, SLTT	Intermediate	3	3

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Protect and Defend	
				Specialty Areas	Work Roles
IMR 205 - Web and Email Server Attacks	Participants will be introduced to common web and email vulnerabilities, as well as the technologies of encryption and authentication to enhance web and email security. This exercise uses a hands-on approach to facilitate realistic technical training and interaction opportunities for learners.	Federal, SLTT	Intermediate	4	4
IMR 206 - DNS Infrastructure Attacks	Working with cybersecurity engineers in a host environment with various software applications, participants will be introduced to common DNS tampering techniques, as well as the technologies of DNS sinkholing to enhance security. Learners will analyze network and host-based artifacts and implement remediation for the identified vulnerabilities.	Federal, SLTT	Intermediate	3	3
Insider Threat Analysis	This course is designed to help insider threat analysts understand data that can be used to prevent, detect, and respond to insider threats by working with data from multiple sources to develop indicators of potential insider activity, as well as strategies for developing and implementing an insider threat analysis and response.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Mapping IT Defense-in-Depth Security Solutions to ICS, Part 1	This training will introduce the defense-in-depth model and cover layers 1 and 2.	Federal, SLTT	Intermediate	2	2
Mapping IT Defense-in-Depth Security Solutions to ICS, Part 2	This training will continue the defense-in-depth model and cover layer 3 - Network Security.	Federal, SLTT	Intermediate	2	2
Root Cause Analysis	This course provides an explanation of root cause analysis for cyber security 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.	Federal, SLTT, Veterans	Intermediate	2	2

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Securing The Network Perimeter	This course covers edge security traffic design, blocking DoS/DDoS traffic, specialized access control lists, routers and firewalls, securing routing protocols, securing traffic prioritization and securing against SPOF.	Federal, SLTT, Veterans	Intermediate	2	2
SiLK Traffic Analysis	This course is designed to teach the analyst how to make network flow analysis a part of their workflow. Students will learn how to use the SiLK network flow analysis tool suite to perform tasks such as querying for records related to a specific incident or indicator, creating sets of indicators for batch analysis, and leveraging network flow to provide basic network situational awareness.	Federal, SLTT, Veterans	Intermediate	2	2
Windows Operating System Security	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.	Federal, SLTT, Veterans, Public	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Wireless Network Security	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.	Federal, SLTT, Veterans	Intermediate	1	1
301 ICS Cybersecurity	This course provides extensive hands-on training on understanding, protecting, and securing ICS from cyber attacks. Trainees will learn about common vulnerabilities and the importance of understanding the environment they protect. Learning the weaknesses of a system will enable trainees to implement the mitigation strategies and institute policies and programs that will provide the defense-in-depth needed for a more secure ICS environment.	Federal, SLTT	Intermediate	2	2
401 ICS Evaluation	This instructor-led course provides hands-on training on how to analyze, evaluate, and document the cybersecurity posture of an organization's ICS to recommend changes. Specifically, It will utilize a multi-step repeatable process, within a simulated ICS environment, that teaches how to analyze cybersecurity weaknesses and threats, evaluate and map findings, document potential mitigations, and provide ongoing resolutions to strengthen the cybersecurity posture.	Federal, SLTT	Intermediate	2	2

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Protect and Defend	
				Specialty Areas	Work Roles
Certified Ethical Hacker (CEHv10)	This course helps prepare students to sit for the EC-Council CEHv10 certification exam. This course helps students broaden their knowledge of advanced network assessment techniques including enumeration, scanning and reconnaissance. This course is designed for the skilled professional to use the same knowledge and tools as a malicious hacker but in an ethical and lawful manner to examine an organization's network security posture.	Federal, SLTT, Veterans	Advanced	2	2
IMR 302 - Cloud Leak: Cloud Leak Cyber Range Challenge	Scenario: Participants must capture network and host-based artifacts from the attack, report the source and extent of a compromise, and provide recommendations for hardening the network against attack and better data hygiene practices.	Federal, SLTT	Advanced	4	4
IMR 303 - Business Email Attack: Business Email Compromise Cyber Range Challenge	Scenario: Your organization receives an announcement that a Business Email Compromise is suspected to have occurred. Participants then use tools on the host environment to investigate the intrusion and uncover evidence. Once data collection is complete, participants submit a briefing and discuss their findings.	Federal, SLTT	Advanced	2	2

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Protect and Defend	
				Specialty Areas	Work Roles
IPv6 Security Essentials	This course begins with a primer of IPv6 addressing and its current deployment state, discusses ICMPv6, DHCPv6, and DNSv6, and concludes with IPv6 Transition Mechanisms, security concerns and management strategies.	Federal, SLTT, Veterans	Advanced	1	1
ISACA Certified Information Security Manager Prep (CISM)	This certification prep self-study resource helps prepare candidates to sit for the management-focused CISM exam. The course includes concepts like Information Security Governance, Information Risk Management and Compliance, Information Security Program Development and Management, and Information Security Incident Management.	Federal, SLTT, Veterans	Advanced	1	1
Linux Operating Systems Security	This course introduces security features and tools available in Linux as well as the considerations, advantages, and disadvantages of using those features. The class 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.	Federal, SLTT, Veterans	Advanced	1	1

Professional Development Training

◄ Prev Next ►

Protect and Defend

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Protect and Defend	
				Specialty Areas	Work Roles
Radio Frequency Identification (RFID) Security	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.	Federal, SLTT, Veterans	Advanced	1	1

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
(ISC)^{2} (TM) Systems Security Certified Practitioner	This course serves as a preparation for the Systems Security Certified Practitioner (SSCP) certification exam, by demonstrating advanced technical skills and knowledge required to implement and administer infrastructure using security best practices, policies, and procedures.	Federal, SLTT, Veterans	Entry	1	1
101 Introduction to Control Systems Cybersecurity	This course introduces students to the basics of Industrial Control Systems (ICS) cybersecurity. This includes a comparative analysis of IT and ICS architectures, understanding risk in terms of consequence, security vulnerabilities within ICS environments, and effective cyber risk mitigation strategies for the Control System domain.	Federal, SLTT	Entry	1	2
Access Control	What is Access Control? Why does this matter? What is a High Value Asset (HVA)? What issue did DHS find? Guidance for protecting HVAs	Federal, SLTT	Entry	1	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Advanced Windows Scripting	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.	Federal, SLTT, Veterans	Entry	1	1
Authentication	Why does HVA authentication matter? What does it mean to you? How can you protect your organization?	Federal, SLTT	Entry	1	2
CDM 141 - Introduction to the New CDM Agency Dashboard	This course is a recording of a virtual two-hour course which is the first of six webinars. This course provides participants with the essential knowledge of the ES-2 version of the CDM Agency Dashboard. It explains basic features and navigation within the environment, and includes demonstrations using the new CDM Agency Dashboard to identify and report on vulnerabilities.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
CDM Agency Dashboard: The CONOPS and Beyond	Learn about the Concept of Operations (CONOPS) for the Agency CDM Dashboard. Mr. Willie Crenshaw, Program Executive for CDM, National Aeronautics and Space Administration (NASA), and Mr. Mark Singer, Guidance and Planning Team Lead for Cybersecurity Governance, Federal Network Resilience Division, review the highlights of the CDM Agency Dashboard CONOPS, what features are included through CDM Release 6, and how agencies can take full advantage of Release 6 features.	Federal, SLTT	Entry	1	2
Cloud Security - What Leaders Need to Know	This course features National Defense University Professor Robert Richardson who discusses important security and oversight requirements for commercial cloud solutions.	Federal, SLTT, Veterans	Entry	3	5
Coding 101	This course focuses on the basics of computer programming and how to give a machine a set of instructions to produce a desired behavior. This course also 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 a fully functional code.	Federal, SLTT, Veterans, Public	Entry	5	5

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Critical Infrastructure Protection	This course discusses 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.	Federal, SLTT, Veterans, Public	Entry	4	4
Cybersecurity Practices for Industrial Control Systems (100W)	This training will cover standard cybersecurity practices with information specific to industrial control systems (ICS). It highlights the type of information an adversary may view as valuable. The training provides tools to recognize potential weaknesses in daily operations, as well as effective techniques to address those weaknesses.	Federal, SLTT	Entry	2	3
DB Evaluations using AppDetectivePro and dbProtect	This course introduces students to basic database security concepts, methodologies, and tools such as AppDetectivePRO and DbProtect. These 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 that could lead to cyber attacks.	Federal, SLTT, Veterans	Entry	2	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Don't Wake Up to a Ransomware Attack	This course provides essential knowledge and reviews real-life examples of these attacks to help you and your organization to prevent, mitigate, and respond to the ever-evolving threat of ransomware.	Federal, SLTT, Veterans	Entry	4	6
Dynamic Testing Using HPE Webinspect	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 from both a developer and cyber security professional perspective.	Federal, SLTT, Veterans	Entry	2	2
Elections and IT - Embrace your role as a Manager	The course serves as an overview of information technology and how to ensure security is included in the planning, procuring, designing, implementing, and maintaining of interconnected electronic election systems, including public-facing websites. The content introduces the key concepts of identifying vulnerabilities and how to protect election systems from internal and external threats and provides information on cybersecurity resources available from the EAC and DHS.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Enterprise Risk Management	What is ERM? What is a High Value Asset? Why does ERM matter to HVAs? What does ERM mean to HVAs? How should Federal agencies plan to address this finding?	Federal, SLTT	Entry	1	2
Fundamentals of Cyber Risk Management	Fundamentals of Cyber Risk Management covers key concepts, issues, and considerations for managing risk. Discussions include identifying critical assets and operations, risk assessment and analysis methodologies, risk management frameworks, and how to determine threats to your business function, mitigation strategies, and response and recovery.	Federal, SLTT, Veterans	Entry	1	1
Hacker 101 and Secure Coding	The Hacker 101 course is designed to introduce students to the basic concepts of hacker activity, understand how to combat such activities, and learn how to reduce the risk of cyber-attacks by understanding the hacker mindset. The course covers reconnaissance before a hacker attack, exploiting a system and performing an attack, and post-exploit activities.	Federal, SLTT, Veterans, Public	Entry	3	3

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
How Data Consistency Impacts CDM	Learn more about how data consistency impacts CDM from Mr. Rick McMaster, CDM Program Management Office. This webinar includes open discussions with attendees to better understand challenges and lessons learned.	Federal, SLTT	Entry	1	2
How Identity, Credential, and Access Management (ICAM) Protects Your Agencies' Assets	Learn about the importance of ICAM in the context of the CDM Program and the "life cycle" of agencies' employees as they join, move in, then leave an organization. A one-hour webinar on ICAM -the credential management issues that arise during CDM Phase 2, how ICAM factors into cloud computing, and the zero-trust approach to access control.	Federal, SLTT	Entry	1	2
How to Address the Threat of Ransomware Attacks	What is Ransomware? How it works? What are the signs of infection? What can you do?	Federal, SLTT	Entry	1	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
IMR 001 - Ransomware	The course includes an overview of ransomware attacks and how threat actors compromise systems to lock out legitimate users and exfiltrate data. Expert facilitators outline the process of investigation, intrusion, and compromise; and how threat hunters and network defenders observe, diagnose, and mitigate attack activity as they proceed through the scenario.	Federal, SLTT	Entry	4	6
IMR 002 - Cloud Security	This course puts you front and center for a live, two-hour red team/ blue team cyber range demonstration of a Business Email Compromise cyberattack. Be in the room where it happens, guided by expert engineers through the attack and defense strategy of each side to impart understanding and essential takeaways that prepare you and your organization for what it takes to orchestrate an effective response to a real-time cyberattack. .	Federal, SLTT	Entry	4	6
IMR 003 - Business Email Compromise	This course puts you front and center for a live, two-hour red team/ blue team cyber range demonstration of a Business Email Compromise cyberattack. Be in the room where it happens, guided by expert engineers through the attack and defense strategy of each side to impart understanding and essential takeaways that prepare you and your organization for what it takes to orchestrate an effective response to a real-time cyberattack.	Federal, SLTT	Entry	3	5

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
IMR 102 - Cloud-based server attacks: Don't Get Caught in the Storm	An overview of cloud computing and its associated security vulnerabilities, common signs of a cloud server attack and how to respond to suspicious activity, CISA guidance and best practices to mitigate cloud server vulnerabilities, secure cloud systems, and block threat activity, case studies demonstrating the impacts of cloud attacks, including major data breaches	Federal, SLTT	Entry	4	6
IMR 103 - Business Email Compromise: Preventing Business Email Attacks	An overview of business email compromise, phishing, and its impact on organizations. Learn how to identify a business email attack, mitigate the likelihood and impact of BEC through best practices, and respond and recover funds in the event of an attack.	Federal, SLTT	Entry	3	5
IMR 104 - Internet-Accessible System Vulnerabilities: Don't Let Cyber Criminals Steal Your Connections	Internet-accessible systems have become the backbone of modern business and communication infrastructure, from smartphones to web applications such as Outlook to the explosive growth of the "Internet of Things" (IoT). Each of these systems and devices, however, can be targeted by threat actors and used to conduct malicious activity if they are unsecured.	Federal, SLTT	Entry	3	5

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
IMR 105 - Web and Email Server Attacks: Securing Web and Email Servers	Web and email servers are the workhorses of the Internet: we couldn't run government, businesses, or our personal lives without them! However, the information exchanged through web and email servers can offer a tempting target for cyber attackers. Key Guidance for Organizations: CISA provides resources and best practices to help individuals and organizations secure their web and email infrastructure.	Federal, SLTT	Entry	2	2
ISCM E-Learning Module	This course provide introductory information on the importance of building an ISCM strategy, how ISCM integrates with an organization's Enterprise Risk Management (ERM) strategy, and ISCM program management and execution	Federal, SLTT	Entry	1	2
Learn How CDM's AWARE Scoring Can Help You Reduce Cyber Risk	Learn how AWARE works, and how it can be used to reduce risks across the federal enterprise - an overview of the scoring methodology behind AWARE, and what you need to do to improve your agency's score. Insights on how AWARE could evolve as agencies gain more experience with CDM to support information security continuous monitoring policies	Federal, SLTT	Entry	1	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
LEGACY CDM Agency Dashboard Asset Discovery Bootcamp (CDM110)	This in-person course incorporates the first three CDM Agency Dashboard training courses into one two-day event and allows additional time for hands-on exercises and questions. The class includes all content from: Introduction to Creating Queries & Reports; Using Measurement & Metrics of Hardware & Software Assets; Using the CDM Agency Dashboard to Drive Your Vulnerability Management Work Plan.	Federal, SLTT, Veterans	Entry	1	2
LEGACY Introduction to Creating Queries & Reports Using the CDM Agency Dashboard (CDM102)	This course provides participants with the basic knowledge of continuous monitoring concepts. It includes four live demonstrations using the search, query, and reporting capabilities of the CDM Agency Dashboard to identify and report on vulnerabilities.	Federal, SLTT, Veterans	Entry	1	2
LEGACY Using Measurements & Metrics of Hardware & Software Assets with the CDM Agency Dashboard (CDM103)	This course presents an overview of how the dashboard provides visibility into the metrics and measurements needed for a continuous monitoring program; explains how to create queries for HW and SW assets; and introduces a framework for using data reports to inform risk-based decision-making.	Federal, SLTT, Veterans	Entry	1	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Securely Provision: Specialty Areas	NICE Framework Mapping: Securely Provision: Work Roles
LEGACY Using the CDM Agency Dashboard to Drive Your Vulnerability Management Work Plan	This course introduces participants to CDM Agency-Wide Adaptive Risk Enumeration (AWARE).	Federal, SLTT, Veterans	Entry	1	2
Let's Talk About Aware...	In this 17-minute episode, David Otto, a Risk Management Subject Matter Expert with the Continuous Diagnostics & Mitigation Program, talks about how agencies can optimize the use of Agency-Wide Adaptive Risk Enumeration (AWARE) – an algorithm tied into the CDM Federal Dashboard that helps agencies measure risk. Other topics include how agencies can interpret and socialize their AWARE results and how AWARE and the Risk Management Framework complement each other to mitigate risk.	Federal, SLTT	Entry	1	2
Malware Defense	What is Malware? Why does it matter? What this means to You. What is a High Value Asset (HVA). What Issues did DHS find? Protecting HVAs.	Federal, SLTT	Entry	1	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Measuring What Matters: Security Metrics Workshop	This workshop focuses on how to measure the right things in order to make informed management decisions, take the appropriate actions, and change behaviors. Students will learn how to refine a strategic or business objective that meets that S.M.A.R.T.E.R. criteria: Specific, Measurable, Achievable, Relevant, Time-bound, Evaluated, Reviewed, and can be used to initiate the Goal - Question - Indicator - Metric (GQIM) process.	Federal, SLTT, Veterans	Entry	1	1
Network Layer 1 & 2 Troubleshooting	This course reviews troubleshooting methods used in Layer 1 and Layer 2 of the OSI Model. 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.	Federal, SLTT, Veterans	Entry	1	1
New CDM Agency Dashboard Videos (8 Videos)	These short videos (5-11 minutes) of the new CDM Agency Dashboard will provide a foundation level of knowledge and background that will help end users of the dashboard prepare for training demonstrations and hands-on activities, as well as the implementation of the new dashboard.	Federal, SLTT, Veterans	Entry	2	6

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Patch Management	What is a High Value Asset? Why is this Patch Management finding important? What types of challenges do organizations face with Patch Management? What steps should your organization take to respond to this finding?	Federal, SLTT	Entry	1	2
Ransomware	How to Address the Threat of Ransomware Attacks. What is Ransomware? How it works? What are the signs of infection? What can you do?	Federal, SLTT	Entry	1	2
Reverse Engineering	This course focuses on the basics of reverse engineering, the process of analyzing a technology to determine how it was designed or how it operates. By starting with a finished product, in this case computer software, and working backwards to determine its component parts.	Federal, SLTT, Veterans, Public	Entry	2	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Risk Management Framework for Leaders	This webinar discusses key leadership decisions to implement the NIST Risk Management Framework (RMF). RMF is a risk-based approach to implement security within an existing enterprise - it is leadership's responsibility to ensure adequate and effective system security.	Federal, SLTT, Veterans	Entry	3	5
Securing Internet-Accessible Systems	This course focuses on Internet-accessible systems or "Internet of Things" (IoT). These systems and devices can be targeted by threat actors and used to conduct malicious activity if they are unsecured, or worse, these systems can leave vulnerabilities and sensitive information open to exploitation if not properly configured and maintained. This course explains the vulnerabilities of internet-accessible systems and how to prepare for, mitigate, and respond to a potential attack.	Federal, SLTT, Veterans	Entry	2	3
Static Code Analysis Using HPE Fortify	Using HPE Fortify 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 Fortify is used to identify and remove Common Weakness Enumeration (CWE) from applications in which the source code is available.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Static Code Analysis Using Synopsis Coverity	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.	Federal, SLTT, Veterans	Entry	2	2
Supply Chain Assurance Using Sonatype Nexus	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 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.	Federal, SLTT, Veterans	Entry	2	2
The Election Official as IT Manager	This course focuses on why Election Officials must view themselves as IT systems managers and introduces the knowledge and skills necessary to effectively function as an IT manager. The course includes a review of Election Systems, Election Night Reporting, and Interconnected Election Systems vulnerabilities and liabilities. The content also covers Social Media and Website best practices, vulnerabilities, and liabilities, and addresses Procuring IT, Vendor Selection, Testing and Audits, and Security Measures.	Federal, SLTT, Veterans	Entry	1	1

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Understanding DNS Attacks	This course provides key information you need to know to protect yourself and your organization from DNS infrastructure tampering including common vulnerabilities, how to identify a potential attack, and guidance and best practices to mitigate the likelihood and impact of a successful DNS attack.	Federal, SLTT, Veterans	Entry	4	6
Understanding Web and Email Server Security	Understanding Web and Email Server Security	Federal, SLTT, Veterans	Entry	3	5
Using the CDM Agency Dashboard to Combat WannaCry Ransomware	This 15-minute video explains how a Federal Agency can use the CDM Agency dashboard to identify and mitigate system vulnerabilities that are exploited by the WannaCry Ransomware malware. The video demonstrates tasks that can be carried out in the CDM Agency dashboard to manage risks to agency systems and information that might be otherwise taken advantage of by this negative threat	Federal, SLTT	Entry	1	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Vulnerability Management Using Drupal	The 10-minute video describes how the CDM program can be used to identify and remediate cybersecurity risks through vulnerability management using the example of Drupal Security Alerts.	Federal, SLTT	Entry	1	2
201 Intermediate Cybersecurity for Industrial Control Systems, Part 1	This course provides technical instruction on the protection of Industrial Control Systems using offensive and defensive methods. Attendees will recognize how cyber attacks are launched, why they work, and mitigation strategies to increase the cybersecurity posture of their Control System networks. This course acts as a prerequisite for the next course, Intermediate Cybersecurity for Industrial Control Systems	Federal, SLTT	Intermediate	1	2
202 Intermediate Cybersecurity for Industrial Control Systems, Part 2	This course provides a brief review of Industrial Control Systems security. This includes a comparative analysis of IT and control system architectures, security vulnerabilities, and mitigation strategies unique to the Control System domain. Because this course is hands-on, students will get a deeper understanding of how the various tools work. Accompanying this course is a sample Process Control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions.	Federal, SLTT	Intermediate	1	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Cloud Computing Security	The course explores guidance from the Cloud Security Alliance (CSA), National Institute of Standards and Technology (NIST), National Security Agency (NSA), and several Cloud Service Providers (CSPs). Topics will cover cloud security risks and threats, basic operations, incident response considerations, along with application, data and infrastructure security concepts as well as demonstrations of cloud provider tools and capabilities.	Federal, SLTT, Veterans, Public	Intermediate	2	2
Common ICS Components (210W-03)	This course covers the common components found in Industrial Control Systems (ICS). It reviews the components found in most ICS.	Federal, SLTT	Intermediate	1	2
Current Trends (Threat) (210W-06)	Risk is a function of threat, vulnerability, and consequence. The most complex attribute is threat because it can be intentional or unintentional, natural or man-made. When trying to develop defensive strategies to protect controls systems, it is important to understand the threat landscape in order for appropriate countermeasures or compensating controls to be deployed.	Federal, SLTT	Intermediate	1	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Current Trends (Vulnerabilities) (210W-07)	In this course, we examine some of the current trends in cybersecurity vulnerabilities that contribute directly to cyber risk in Industrial Control Systems (ICSs). The goal is to identify the root causes and their associated countermeasures that can be used to protect control systems.	Federal, SLTT	Intermediate	1	2
Cyber Supply Chain Risk Management	This course focuses on cyber supply chain risk management, also known as C-SCRM, and the role it plays within our society today. This course will explain how to securely provision, analyze, oversee and govern, protect and defend a supply chain.	Federal, SLTT, Veterans, Public	Intermediate	2	2
Cybersecurity Risk (210W-05)	This course is designed to help you gain a better understanding of cyber risk, how it is defined in the context of ICS security, and the factors that contribute to risk. This will empower you to develop cybersecurity strategies that align directly with the ICS environment. Also, learn how IT-based countermeasures can be customized to accommodate for the uniqueness of ICS architectures.	Federal, SLTT	Intermediate	1	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping: Securely Provision: Specialty Areas	NICE Framework Mapping: Securely Provision: Work Roles
Differences in Deployments of Industrial Control Systems (210W-01)	This course discusses what, where, and how industrial control systems (ICSs) are used and describes some of specific examples of how ICSs work in real-life situations.	Federal, SLTT	Intermediate	2	4
Enterprise Cybersecurity Operations	This course highlights technical knowledge and skills required for implementing secure solutions in the enterprise. A broad spectrum of disciplines is covered to aid practitioners in applying frameworks and controls to improve the security posture while supporting the business mission.	Federal, SLTT, Veterans	Intermediate	2	2
FedRAMP: A Leader's Dashboard for Compliance	In this hour-long webinar National Defense University Professor Roxanne Everetts discusses some key leadership decisions around using Federal Risk and Authorization Management Program (FedRAMP) solutions. FedRAMP is a unique government cloud - it is a combination of cloud security, cybersecurity, and risk management.	Federal, SLTT, Veterans	Intermediate	2	3

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
ICS Cybersecurity Consequences (210W-08)	A cyber attack that results in the release of a toxic chemical and kills 10 people is more significant than a cyber attack that temporarily disables the HVAC in a control – or is it? This course will help you better understand the impacts of cyber based attack can have on an ICS and provide you with different ways of looking at the potential consequences of three types of events.	Federal, SLTT	Intermediate	1	2
IMR 204 - Vulnerabilities of Internet-Accessible Systems: Defending Internet-Accessible Systems Cyber Range Training	Four activities that explore the following aspects: network mapping, identifying and remediating vulnerabilities in internet-accessible systems, and resolving password spraying attacks. Participants will use tools and work with cybersecurity engineers in a host environment with a sample hygiene assessment report to investigate the network, prioritize vulnerabilities, and apply firewall rules to your network.	Federal, SLTT	Intermediate	2	3
IMR 205 - Web and Email Server Attacks	Participants will be introduced to common web and email vulnerabilities, as well as the technologies of encryption and authentication to enhance web and email security. This exercise uses a hands-on approach to facilitate realistic technical training and interaction opportunities for learners.	Federal, SLTT	Intermediate	3	4

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
IMR 206 - DNS Infrastructure Attacks	Working with cybersecurity engineers in a host environment with various software applications, participants will be introduced to common DNS tampering techniques, as well as the technologies of DNS sinkholing to enhance security. Learners will analyze network and host-based artifacts and implement remediation for the identified vulnerabilities.	Federal, SLTT	Intermediate	4	6
Securing Infrastructure Devices	This course covers physical security, operating system security, management traffic security, device service hardening, securing management services and device access privileges.	Federal, SLTT, Veterans	Intermediate	1	1
Software Assurance Executive (SAE) Course	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.	Federal, SLTT, Veterans	Intermediate	1	1

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
Wireless Network Security	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.	Federal, SLTT, Veterans	Intermediate	1	1
(ISC)² ™ CISSP (R) Certification Prep	This 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.	Federal, SLTT, Veterans	Advanced	1	1
301 ICS Cybersecurity	This course provides extensive hands-on training on understanding, protecting, and securing Industrial Control Systems (ICS) from cyber attacks and includes a Red Team/Blue Team exercise conducted within an actual Control Systems environment. Trainees will learn about common vulnerabilities and the importance of understanding the environment they are tasked to protect. Learning the weaknesses of a system will enable trainees to implement the mitigation strategies and institute policies and programs that will provide the defense-in-depth needed to ensure a more secure ICS environment.	Federal, SLTT	Advanced	1	2

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
401 ICS Evaluation	This instructor-led 5-day course provides hands-on training on how to analyze, evaluate, and document the cybersecurity posture of an organization's Industrial Control Systems (ICS) for the purpose of identifying recommended changes. Specifically, the course will utilize a multi-step repeatable process, within a simulated ICS environment, that teaches how to analyze cybersecurity weaknesses and threats, evaluate and map findings, document potential mitigations, and provide ongoing resolutions to strengthen the cybersecurity posture.	Federal, SLTT	Advanced	1	2
DNSSEC Training Workshop	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. Topics include DNSSEC introduction, DNSSEC mechanisms, signing a zone, delegation signer (DS) RRs, setting up a secure resolver, server operational considerations and DNSSEC conclusions.	Federal, SLTT, Veterans	Advanced	1	1
IMR 302 - Cloud Leak: Cloud Leak Cyber Range Challenge	Scenario: Participants must capture network and host-based artifacts from the attack, report the source and extent of a compromise, and provide recommendations for hardening the network against attack and better data hygiene practices.	Federal, SLTT	Advanced	4	6

Professional Development Training

◄ Prev Next ►

Securely Provision

Course	Description	Audience	Proficiency Level	NICE Framework Mapping	
				Securely Provision	
				Specialty Areas	Work Roles
IMR 303 - Business Email Attack: Business Email Compromise Cyber Range Challenge	Scenario: Your organization receives an announcement that a Business Email Compromise is suspected to have occurred. Participants then use tools on the host environment to investigate the intrusion and uncover evidence. Once data collection is complete, participants submit a briefing and discuss their findings.	Federal, SLTT	Advanced	3	5
IPv6 Security Essentials	This course begins with a primer of IPv6 addressing and its current deployment state, discusses ICMPv6, DHCPv6, and DNSv6, and concludes with IPv6 Transition Mechanisms, security concerns and management strategies.	Federal, SLTT, Veterans	Advanced	1	1
Security and DNS	This course discusses name resolution principles, name resolution and security, DNS security standards, securing zone transfers with TSIG, and DNSSEC principles, implementation and resources.	Federal, SLTT, Veterans	Advanced	1	1

CISA Hands-On

CISA has multiple ways to gain practical cybersecurity experience. Hands-on experience is just as important as classroom training. Our innovations lab took things to a whole new level to give beginner- through advanced-level cyber professionals opportunities to polish their skills in an interactive and competitive environment.

Cybersecurity Competitions and Games

Cybersecurity competitions and gamification are creative ways to help you put your cybersecurity skills to the test. Competitions and games are not the same thing, but there are some similarities.

- Competitions and games all range in skill levels and can be team-based/multi-player or individual
- Both offer hands-on experience and enable users to utilize cybersecurity skills and decision-making processes in a fun way
- Cybersecurity competitions and games can be used as training and recruitment tools by employers because they allow employees and candidates to demonstrate their cybersecurity skills

Federal Executive Skilling

CISA understands the importance for all federal leaders to build their cybersecurity skillset. The Federal Executive Cybersecurity Skills course is for non-cybersecurity professionals and provides specialized training for senior executive leaders to better understand cyber attacks and how to address cyber threats.

- The Federal Executive Cybersecurity Skills course began in 2020
- The course is for non-cyber federal senior leaders and takes place twice a week for five weeks
- Course size is limited

Competitions

◄ Prev Next ►

Cybersecurity Competitions

Cybersecurity competitions are interactive, scenario-based exercises – in person or virtual – where individuals or teams engage in cybersecurity activities including methods, practices, strategy, policy, and ethics. Competitions encourage players to practice, hone cybersecurity Skills, and build confidence in a controlled, real-world environment and are available for all ages and levels.

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

The President's Cup Cybersecurity Competition

President's Cup is a national cyber event aiming to identify, challenge, and reward the best cybersecurity talent in the federal workforce. Held annually, the President's Cup consists of individual and team challenges focusing on areas across the NICE Framework.

Each year CISA livestream broadcasts the President's Cup final round. You can watch the video from the previous years' livestreams at any time on YouTube.

2020 Final Team Competition

2019 Final Team Competition

Competitions

◄ Prev Next ►

Cybersecurity Competitions

Cybersecurity competitions are interactive, scenario-based exercises – in person or virtual – where individuals or teams engage in cybersecurity activities including methods, practices, strategy, policy, and ethics. Competitions encourage players to practice, hone cybersecurity Skills, and build confidence in a controlled, real-world environment and are available for all ages and levels.

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

The President's Cup Practice Area

CISA created a practice area where sample challenges can be accessed at any time in a friendly and low-stakes environment. Register with an email address from any of the domains listed below and join the fun!

.gov | .mil | csosa.fed.us | manufacturingusa.com | mfgusa.com | hearttruth.net | hearttruth.org | medlineplus.net | nlm.net | phpartners.org | thehearttruth.com | thehearttruth.net | thehearttruth.org | treasury.fed.us | usmma.edu | usna.edu | usafa.edu | afit.edu | nps.edu | shopvcs.com | vacloud.us | vaftl.us | vaglaid.org | vamobile.us | vapulse.net | veteranscrisisline.net | veteranshealthlibrary.org | frb.fed.us | fs.fed.us | usda.net | usps.com | westpoint.edu | sei.cmu.edu

Games

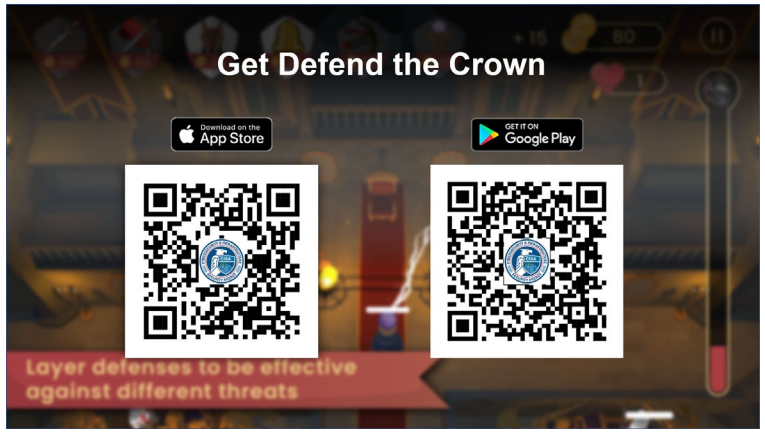
Cybersecurity games are easily accessible and adoptable tools that help increase cybersecurity workforce development capacity by sparking interest in a fun and engaging way. This approach blends an element of fun with learning objectives. CISA partnered with Pacific Northwest National Laboratory (PNNL) to create a series of games to be released via the Apple AppStore and Google Play in 2021.

Defend the Crown

The first game, released by CISA in June of 2021, is designed for early career, non-technical cybersecurity professionals. The player must protect their castle from invasion by deploying defenses. The game is designed to educate on cybersecurity attack phases, vulnerabilities, defenses, and mitigations.

Example NICE framework ties for Defend the Crown:

- K0005 Knowledge of cyber threats and vulnerabilities
- K0110 Knowledge of adversarial tactics, techniques, and procedures
- K0112 Knowledge of defense-in-depth principles and network security architecture
- K0362 Knowledge of attack methods and techniques (DDoS, Brute force, spoofing, etc.)



Executive Skilling

Federal Executive Cybersecurity Skills course from CISA and FEI

CISA and the Office of Personnel Management (OPM) Center for Leadership Development, Federal Executive Institute (FEI) have partnered to create a specialized training for non-cyber federal senior leaders to help them identify and respond to cyber-attacks within their organization. The course includes ten sessions of 60-120 minutes each over five weeks and provides an introduction to fundamental concepts in cyber policy and security from the perspective of a federal executive. Participants hold the rank of Senior Executive Service (SES) or Senior Leader. The course is primarily intended for non-technical, non-cyber federal executives who would not routinely encounter these types of issues within their typical duties. The Federal Executive Cybersecurity Skills course was created in 2020 and is back by popular demand with take-aways from recent events incorporated into the curriculum.

Topics include:

- Cybersecurity Fundamentals
- Cybersecurity Risk Management
- Cyber Readiness
- Leading Through Crisis

For more information, contact education@cisa.dhs.gov.

Coming Soon

CISA is looking into other competitions and hands-on activities that will help entry to advanced cybersecurity professionals practice and test proficiency levels in a variety of Tasks and KSAs. As we explore more hands-on opportunities that will benefit the community, we intend on providing updates when and where possible.

In 2021, CISA also plans to release Network Collapse, a game aimed for middle schoolers in August, and a third game for high school students in the fall. The games will include a variety of topics, including Internet of Things (IoT) security, computer networking, and general cybersecurity awareness. We can't wait to share these with the world. For more information, please visit www.cisa.gov/cybergames.

Certifications

◄ Prev Next ►

Entry

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Associate of (ISC)^2

Covers the following: Security and Risk Management, Asset Security, Security Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security. This certification is compatible for O&M NICE categories.

Prerequisites?
No

Learn More

Certified Authorization Professional (CAP)

Measures the Knowledge, Skills and Abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation.

Prerequisites?
Yes

Learn More Prep Materials on FedVTE

Certifications

◄ Prev Next ►

Entry

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified Information Privacy Professional (CIPP)

Provides a foundational understanding of broad global concepts of privacy and data protection law and practice, plus knowledge of the following components within your concentration:

- Jurisdictional laws, regulations and enforcement models, or rules and standards
- Essential privacy concepts and principals
- Legal requirements for handling and transferring data.

Prerequisites?
No

Learn More

Cisco Certified Network Associate (CCNA)

To earn CCNA certification, you pass one exam that covers a broad range of fundamentals for IT careers, based on the latest networking technologies, security, and automation and programmability skills and job roles.

Prerequisites?
Yes

Learn More | Prep Materials on FedVTE

Certifications

◄ Prev Next ►

Entry

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

CompTIA Security+

Validates foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management.

Prerequisites?
Yes

Learn More

Prep Materials on FedVTE

Systems Security Certified Practitioner (SSCP)

For those with proven technical skills and practical security knowledge in hands-on operational IT roles. Indicates a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certificate of Cloud Security Knowledge (CCSK)

Provides evidence that an individual has successfully completed an examination covering the key concepts of the CSA Guidance, the CSA CCM, and the ENISA whitepaper.

Prerequisites?
No

Learn More

Certified Ethical Hacker (CEH)

This credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor- neutral perspective. Students will be immersed into a hands-on environment where they will be shown how to conduct ethical hacking. They will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! They will scan, test, hack and secure their own systems.

Prerequisites?
Yes

Learn More Prep Materials on FedVTE

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified Forensic Examiner (GCFE)

For professionals working or interested in the information security, legal and law enforcement industries with a need to understand computer forensic analysis. The GIAC Certified Forensic Examiner certification focuses on core skills required to collect and analyze data from Windows computer systems.

Prerequisites?
No

Learn More

Certified Identity and Access Management (CIAM)

Ensures competency in one of the most important disciplines of information security which aims to manage user identities and access to enterprise resources and data. IAM governance and programs including policies, processes, and technologies manage user identities and define what they can access and do within a system through identification, authentication, approved access rights, and activity monitoring.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified in Risk and Information Systems Control (CRISC)

Prepares IT professionals for the unique challenges of IT and enterprise risk management and positions them to become strategic partners to the enterprise.

Prerequisites?
Yes

Learn More

Certified Incident Handler (GCIH)

Focuses on detecting, responding, and resolving computer security incidents and covers the following security techniques:

- The steps of the incident handling process
- Detecting malicious applications and network activity
- Common attack techniques that compromise hosts
- Detecting and analyzing system and network vulnerabilities
- Continuous process improvement by discovering the root causes of incidents

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified Systems Engineering Professional (CSEP)

For practicing Systems Engineers with more than five years of systems engineering professional work experience. This will indicate that the individual has a balance between the depth and breadth of SE experience having performed in some, but not all, of the SE function areas.

Prerequisites?
Yes

Learn More

Certified Test and Evaluation Professional (CTEP)

Designed to measure the knowledge, skills, and abilities required to perform competently as a test and evaluation professional.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Cisco Certified Network Professional – Routing and Switching (CCNP)

Validates the ability to plan, implement, verify and troubleshoot local and wide-area enterprise networks and work collaboratively with specialists on advanced security, voice, wireless and video solutions. The CCNP Routing and Switching certification is appropriate for those with at least one year of networking experience who are ready to advance their skills and work independently on complex network solutions.

Prerequisites?
Yes

Learn More

Cisco Certified Network Professional Security (CCNP)

A three-year certification program for Cisco network security engineers who have the necessary skills to test, deploy, configure, maintain, and troubleshoot the Cisco network security appliances and Cisco IOS Software devices that establish the security posture of the network.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Computer Hacking Forensic Investigator (CHFI)

Fortifies the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personal, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.

Prerequisites?
Yes

Learn More

Global Industrial Cyber Security Professional (GICSP)

Will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments.

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Information Security Professional (GISP)

This serves as a baseline cybersecurity certification. It covers many of the same categories as the CISSP but does not have the same years of professional experience required. The topics are all related to cybersecurity and discuss defense in depth, Windows security, Linux security, wireless security, etc.

Prerequisites?
Yes

Learn More

Juniper Networks Certified Internet Specialist Security (JNCIS-SEC)

Designed for experienced networking professionals with intermediate knowledge of the Juniper Networks Junos OS for SRX Series devices, this written exam verifies the candidate's understanding of security technologies and related platform configuration and troubleshooting skills.

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

(Lean) Six Sigma Green Belt (ICGB)

An ICGB possesses an understanding of all aspects of the Lean Six Sigma Method including competence in subject matters contained within the phases of Define, Measure, Analyze, Improve and Control (DMAIC). They understand how to implement, perform, interpret and apply Lean Six Sigma at a high level of proficiency.

Prerequisites?
No

Learn More

Microsoft Certified Solutions Expert (MCSE)

This certification has twelve different specialty areas (solutions) in which someone can gain certification: Cloud Platform and Infrastructure; Mobility; Data Management and Analytics; Productivity; Server Infrastructure; Private Cloud; Enterprise Devices and Apps; Data Platform; Business Intelligence; Messaging; Communication; SharePoint (In early 2016, the legacy solution "Desktop Infrastructure" was retired).

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Offensive Security Certified Professional (OSCP)

A hands-on penetration testing certification, requiring holders to successfully attack and penetrate various live machines in a safe lab environment. It is considered more technical than other ethical hacking certifications.

Prerequisites?
Yes

Learn More

Offensive Security Experienced Penetration Tester (OSEP)

An advanced penetration testing course. It builds on the knowledge and techniques taught in Penetration Testing with Kali Linux, teaching students to perform advanced penetration tests against mature organizations with an established security function.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Offensive Security Exploit Developer (OSED)

Teaches students the fundamentals of modern exploit development. It starts with basic buffer overflow attacks and builds into learning the skills needed to crack the critical security mitigations protecting enterprises.

Prerequisites?
Yes

Learn More

Professional Certified Investigator (PCI)

Demonstrates an individual's knowledge and experience in case management, evidence collection, and preparation of reports and testimony to substantiate findings. Those who earn the PCI are ASIS board-certified in investigations.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Red Hat Certified System Administrator (RHCSA)

An IT professional who has earned this certification is able to perform the core system administration skills required in Red Hat Enterprise Linux environments.

Prerequisites?
No

Learn More

RSA Archer Certified Administrator (RSA Archer CA)

An RSA Archer CA is a person who has an IT administrator, Business Analyst, or Project Manager role within an organization. An analysis of the major job functions expected of an RSA Archer CA determined that there are three major areas of job role responsibility: Integration and configuration management of the product; Administering security; Knowledge of the communication features of the product.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

RSA Security Analytics Certified Administrator a.k.a. RSA NetWitness Logs & Network Administrator

An RSA Security Analytics CA is a person who has an IT administrator, IS Analyst, or Security Operations role within an organization. An analysis of the major job functions expected of an RSA Security Analytics CA determined that there are three major areas of job role responsibility: General awareness of the functions and capabilities of the product; Configuration and management of the product; Monitoring and troubleshooting product operation.

Prerequisites?
Yes

Learn More

Tenable Certified Nessus Auditor (TCNA)

Individuals will have distinguished themselves as having in-depth knowledge of the Nessus vulnerability scanner and the underlying technical concepts. Nessus is the industry leader in vulnerability management and assessment. In addition to credentialed and network scanning, this certification covers discovery of assets on an enterprise, creation of scan policies, performance of patch auditing, and evaluation for compliance. Advanced analytics, compliance, and reporting are also covered.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Intermediate

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Tenable Certified Passive Vulnerability Scanner Auditor (TCPA)

Designed for IT security analysts, security consultants, or auditors who wish to use all of the features available with Nessus, and SecurityCenter users that wish to gain an in-depth understanding of Nessus vulnerability scanning and how to create custom scan policies and .audit files to perform configuration auditing. This certification covers: Introduction to PVS; PVS Installation – Windows; PVS Installation – Linux; Introduction to the PVS Interface; Configuring PVS; PVS Deployment; Results; Monitoring; Exporting Results as Reports; PVS with other Software.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Assessing Wireless Networks (GAWN)

Designed for technologists who need to assess the security of wireless networks. This GIAC certification focuses on the different security mechanisms for wireless networks, the tools and techniques used to evaluate and exploit weaknesses, and techniques used to analyze wireless networks. Students will gain experience using tools to assess wireless networks, understand how the tools operate, and weaknesses in protocols that they evaluate.

Prerequisites?
No

Learn More

Certified Chief Information Security Officer (CCISO)

Aims toward top-level information security executives. Covers the following 5 domains: Governance (Policy, Legal & Compliance); IS Management Controls and Auditing Management; Management – Projects and Operations (Projects, Technology & Operations); Information Security Core Competencies; Strategic Planning & Finance.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified Cloud Security Professional (CCSP)

Denotes professionals with deep-seated knowledge and competency derived from hands-on experience with information security and cloud computing. CCSPs indicate cloud security expertise and focus on cloud computing while keeping sensitive data secure.

Prerequisites?
Yes

Learn More

Certified Cyber Forensics Professional (CCFP)

An advanced certification for those who need to adapt their knowledge of cyber forensics to different platforms and scenarios. Those who apply for a CCFP test often have more basic cyber forensics credentials and may have prior experience in law enforcement, business intelligence (BI) or law. Those who have worked with tools like e-discovery or in areas of cybersecurity management are good candidates for a CCFP certification.

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified Enterprise Defender (GCED)

Builds on the security skills measured by the GSEC. It assesses more advanced, technical skills that are needed to defend the enterprise environment and protect an organization as a whole. Knowledge, skills and abilities assessed are taken from the areas of Defensive Network Infrastructure, Packet Analysis, Penetration Testing, Incident Handling, and Malware Removal.

Prerequisites?
No

Learn More

Certified Forensic Analyst (GCFA)

For professionals working in the information security, computer forensics, and incident response fields. This GIAC certification focuses on core skills required to collect and analyze data from Windows and Linux computer systems.

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified in the Governance of Enterprise IT (CGEIT)

Recognizes knowledge and application of enterprise IT governance principles and practices. A CGEIT certified professional demonstrates capability of bringing IT governance into an organization.

Prerequisites?
Yes

Learn More

Certified Information Security Manager (CISM)

A management-focused CISM certification that promotes international security practices and recognizes the individual who manages designs and oversees and assesses an enterprise's information security.

Prerequisites?
Yes

Learn More Prep Materials on FedVTE

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified Information Systems Auditor (CISA)

A certification for IS audit control, assurance and security professionals. Being CISA-certified demonstrates audit experience, skills and knowledge, and capability to assess vulnerabilities, report on compliance and institute controls within the enterprise.

Prerequisites?
Yes

Learn More

Certified Information Systems Security Professional (CISSP)

Ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles.

Prerequisites?
Yes

Learn More

Prep Materials on FedVTE

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified Intrusion Analyst (GCIA)

Validates a practitioner's knowledge of network and host monitoring, traffic analysis, and intrusion detection. GCIA certification holders have the skills needed to configure and monitor intrusion detection systems, and to read, interpret, and analyze network traffic and related log files. This certification covers the following areas: Fundamentals of Traffic Analysis and Application Protocols, Open-Source IDS: Snort and Bro, Network Traffic Forensics and Monitoring.

Prerequisites?
No

Learn More

Certified Penetration Tester (GPEN)

The GIAC Penetration Tester certification validates a practitioner's ability to properly conduct a penetration test, using best practice techniques and methodologies. GPEN certification holders have the knowledge and skills to conduct exploits and engage in detailed reconnaissance, as well as utilize a process-oriented approach to penetration testing projects.

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified Project Management Professional (PMP)

Now including predictive, agile and hybrid approaches, the PMP® demonstrates project leadership experience and expertise in any way of working. Useful for project leaders across industries and helps organizations find the people they need to work smarter and perform better.

Prerequisites?
Yes

Learn More

Certified Project Manager Certification (GCPM)

Designed for security professionals and managers who participate in or lead project teams and wish to demonstrate an understanding of technical project management methodology and implementation.

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified Protection Professional (CPP)

Demonstrates proof of knowledge and management skills in eight key domains of security. Those who earn the CPP are ASIS board-certified in security management.

Prerequisites?
Yes

Learn More

Certified Secure Software Lifecycle Professional (CSSLP)

Certifies proficiency in: Developing an application security program in your organization; Reducing production costs, application vulnerabilities and delivery delays; Enhancing the credibility of your organization and its development team; and Reducing loss of revenue and reputation due to a breach resulting from insecure software.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Certified UNIX Security Administrator (GCUX)

Certifies that individuals have the knowledge, skills and abilities to secure and audit UNIX and Linux systems.

Prerequisites?
No

Learn More

Certified Windows Security Administrator (GCWN)

Provides knowledge and skills needed to configure and manage the security of Microsoft operating systems and applications, including Dynamic Access Control, PKI, IPSec, Group Policy, DNSSEC, RADIUS, BitLocker, Secure Boot, PowerShell, and hardening Windows against malware and persistent adversaries. Candidates should be familiar with Windows 7, Server 2008-R2, Windows 8.1, and Server 2012-R2.

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Cisco Certified Internetwork Expert (CCIE)

Recognizes individuals for network engineering skills and mastery of Cisco products and solutions. The certification is offered in the following tracks: CCIE Routing & Switching; CCIE Collaboration; CCIE Data Center; CCIE Security; CCIE Service Provider; CCIE Wireless; Cisco Expert Level Program.

Prerequisites?
No

Learn More

Critical Controls Certification (GCCC)

This certification ensures that candidates have the knowledge and skills to implement and execute the CIS Critical Controls recommended by the Council on Cybersecurity, and perform audits based on the standard. This is the only certification based on the CIS Controls, a prioritized, risk-based approach to security.

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Expert Systems Engineering Professional (ESEP)

Indicates that the individual has a balance between the depth and breadth of SE experience having performed in many, but not all, of the SE function areas.

Prerequisites?
Yes

Learn More

Exploit Researcher and Advanced Penetration Tester (GXPN)

For security personnel whose job duties involve assessing target networks, systems and applications to find vulnerabilities. The GXPN certifies that candidates have the knowledge, skills, and ability to conduct advanced penetration tests, how to model the abilities of an advanced attacker to find significant security flaws in systems and demonstrate the business risk associated with these flaws.

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

FAC - Program/Project Manager Certification - Level III (FAC-PPM)

This certification program is based upon a competency model of performance outcomes which measures the knowledge, skills and abilities gained by program and project managers through professional training, job experience and continuous learning.

Prerequisites?

Yes

Learn More

FAC - Program/Project Manager Certification - Level III - IT Specialization (FAC-PPM-IT)

This course focuses specifically on managing IT teams, systems, projects, etc. The skill sets that are demonstrated as a result of this certification are relevant to the effective, design, development, delivery, and execution of cybersecurity systems.

Prerequisites?

Yes

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Federal IT Security Professional – Designer (FITSP-D)

This certification is designed to demonstrate the federal workforce member (civilian personnel, military, and contractors) possesses the knowledge of federal information technology (IT) security requirements necessary to successfully design and develop the management, operational, and technical IT security controls for systems owned by, or operated on behalf of, the federal government of the United States.

Prerequisites?
Yes

Learn More

Federal IT Security Professional – Manager (FITSP-M)

This certification is designed to demonstrate the federal workforce member (civilian personnel, military, and contractors) possesses the knowledge of federal information technology (IT) security requirements necessary to successfully manage and oversee the management, operational, and technical IT security controls for systems owned by, or operated on behalf of, the federal government of the United States.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Federal IT Security Professional – Auditor (FITSP-A)

This certification is designed to demonstrate the federal workforce member (civilian personnel, military, and contractors) possesses the knowledge of federal information technology (IT) security requirements necessary to successfully audit and assess the management, operational, and technical IT security controls for systems owned by, or operated on behalf of, the federal government of the United States.

Prerequisites?

Yes

Learn More

Information Systems Security Architecture Professional (CISSP-ISSAP)

For CISSPs working in positions such as, but not limited to: System architect, Chief technology officer, System and network designer, Business analyst, Chief security officer. The candidate would generally develop, design, or analyze the overall security plan.

Prerequisites?

Yes

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Information Systems Security Engineering Professional (CISSP-ISSEP)

Guide for incorporating security into projects, applications, business processes, and all information systems. For CISSPs working in positions such as, but not limited to: Senior systems engineer, Information assurance systems engineer, Information assurance officer, Information assurance analyst; Senior security analyst.

Prerequisites?

Yes

Learn More

Prep Materials on FedVTE

Information Systems Security Management Professional (CISSP-ISSMP)

Shows an individual excels at establishing, presenting and governing information security programs. Also demonstrates deep management and leadership skills leading incident handling and/or a breach mitigation team.

Prerequisites?

Yes

Learn More

Prep Materials on FedVTE

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

ITIL Expert Level

Aimed at those who are interested in demonstrating knowledge of the ITIL Scheme in its entirety. The certificate is awarded to candidates who have achieved a range of ITIL certifications and have achieved a well rounded, superior knowledge and skills base in ITIL Best Practices.

Prerequisites?
Yes

Learn More

ITIL Master Level

Validates your ability to apply the principles, methods and techniques from ITIL in the workplace. To achieve the ITIL Master Qualification, you must be able to explain and justify how you have personally selected and applied a range of knowledge, principles, methods and techniques from ITIL and supporting management techniques, to achieve desired business outcomes in one or more practical assignments.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Juniper Networks Certified Expert – Enterprise Routing and Switching (JNCIE-ENT)

This exam is designed to validate the networking professionals' ability to deploy, configure, manage and troubleshoot Junos-based enterprise routing and switching platforms. Throughout this 8-hour practical exam, candidates will build an enterprise network infrastructure consisting of multiple routers and switching devices.

Prerequisites?
Yes

Learn More

Juniper Networks Certified Internet Professional (JNCIP-SEC)

Designed for experienced networking professionals with advanced knowledge of the Juniper Networks Junos software for SRX Series devices, this written exam verifies the candidate's understanding of advanced security technologies and related platform configuration and troubleshooting skills.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Law of Data Security and Investigations (GLEG)

Validates a practitioner's knowledge of the law regarding electronically stored and transmitted records. GLEG certification holders have demonstrated knowledge of the law of fraud, crime, policy, contracts, liability, IT security, and active defense.

Prerequisites?
No

Learn More

Lean Six Sigma Black Belt (ICBB)

Ensures employees are knowledgeable in assembling teams for well-defined projects, defining and measuring success, quantitative metric analysis techniques, and process improvement/control. ICBB is a professional who is well versed in the Lean Six Sigma Methodology, who leads improvement projects, typically in a full-time role. A Lean Six Sigma Black Belt possesses a thorough understanding of all aspects within the phases of D-M-A-I-C.

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Licensed Penetration Tester (LPT)

This exam tests the mastery of the skill-sets required to be a true professional penetration tester – Technical Analysis and Report Writing. You will need to demonstrate a mastery of the skills required to conduct a full blackbox penetration test of a network provided to you by EC-Council on our cyber range.

Prerequisites?

Yes

Learn More

Offensive Security Exploitation Expert (OSEE)

Modern exploits for Windows-based platforms require modern bypass methods to circumvent Microsoft's defenses. In Advanced Windows Exploitation (EXP-401), OSEEs can analyze vulnerable software, find problematic code, and develop a functioning exploit for various modern Windows operating systems.

Prerequisites?

Yes

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Offensive Security Web Expert (OSWE)

An advanced web application security certification. OSWEs have a clear and practical understanding of the web application assessment and hacking process. Demonstrated ability to review advanced source code in web apps, identify vulnerabilities, and exploit them.

Prerequisites?
Yes

Learn More

PMI – ACP (Agile Certified Practitioner)

The ACP certification is the fastest growing project management professional credential with improved success rate of projects completed using this methodology.

Prerequisites?
Yes

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Red Hat Certified Engineer (RCHE)

An existing RHCSA who possesses the additional skills, knowledge, and abilities required of a senior system administrator responsible for Red Hat Enterprise Linux® systems.

Prerequisites?
Yes

Learn More

Reverse Engineering Malware (GREM)

Designed for technologists who protect the organization from malicious code. GREM-certified technologists possess the knowledge and skills to reverse- engineer malicious software (malware) that targets common platforms, such as Microsoft Windows and web browsers. These individuals know how to examine inner-workings of malware in the context of forensic investigations, incident response, and Windows system administration

Prerequisites?
No

Learn More

Certifications

◄ Prev Next ►

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

Security Leadership Certification (GSLC)

For security professionals with managerial or supervisory responsibility for information security staff. Candidates will demonstrate an understanding of effective communication and negotiation tactics, managing employee priorities, the use of TCO analysis for proposed solutions and projects, applying due diligence to reduce legal liability and the risk of fraud, operational security (OPSEC) principles, effective change management and incident response programs, an ability to evaluate and manage risk, familiarity with ethical issues pertaining to IT/Information Security, and demonstrate additional technical competencies.

Prerequisites?

No

Learn More

Systems and Network Auditor (GSNA)

This certificate covers the following domains: Auditing Concepts & Methodology; Auditing Networking Devices & Services; Auditing Unix Systems; Auditing Windows Systems; Web Application Security. GSNAs have the knowledge, skills and abilities to apply basic risk analysis techniques and to conduct a technical audit of essential information systems. Technical staff responsible for securing and auditing information systems; auditors who wish to demonstrate technical knowledge of the systems they are responsible for auditing

Prerequisites?

No

Learn More

Certifications

◀ Prev Next ▶

Advanced

Depending on your job function, you may want to consider pursuing a professional certification as another means to mature your competencies. Certifications are also a great way to position yourself to take on new responsibilities. Below are some certifications for consideration that may help you in your career path. These certifications are grouped by proficiency level.

VMWare Certified Design Expert (VCDX)

This certification is achieved through the unique design defense process, where all candidates must submit and successfully defend a production-ready VMware Solution before a panel of veteran VCDX-DCV holders. This process ensures that those who achieve VCDX status are peer-vetted and ready to join an elite group of world-class consulting architects.

Prerequisites?
Yes

Learn More

Web Application Penetration Tester (GAWPT)

This certification measures and individuals understanding of web application exploits and penetration testing methodology.

Prerequisites?
Yes

Learn More

Experience Opportunities

Stretch Opportunities

Stretch opportunities are activities and tasks that go beyond your day-to-day responsibilities. They're meant to "stretch" your capabilities and expand your experience into new areas. Stretch opportunities may require you to step outside of your comfort zone, but you'll reap the benefits as you gain new knowledge and skills. Below are a few examples of stretch opportunities:

- Serve in an acting leadership role if your supervisor or team lead is out of the office
- Volunteer to be the lead for new projects
- Help plan, coordinate, and facilitate meetings and events where you may be exposed to new ideas and stakeholders

Experience Opportunities

Shadowing

Sometimes you need to see things in action to truly understand them. Job shadowing allows you to watch a supervisor or more experienced team member perform job functions in real time. For example, you can job shadow a colleague to learn how to use a software program or tool or a supervisor to gain insight on problem solving, creative thinking, decision making, and engaging partners. If you'd like to participate in a shadowing program, add it to your Career Development Planning Worksheet and talk to your supervisor about your options.

If your department/agency has shadowing programs or opportunities you wish to include, please email us at Education@cisa.dhs.gov.

Experience Opportunities

Rotations & Details

Broaden your skillset and your understanding of the government as a whole by considering a rotation or detail. These are temporary assignments to other Agencies, Departments, Branches, Divisions, and Components to gain new perspectives and insights. There are several programs available to help you enhance your knowledge across the government and learn new skills that you can bring back to your regular duties. Rotations and details are limited and require more upfront planning than other development opportunities, so it's important to talk to your supervisor to coordinate logistics.

The **Joint Duty Program (JDP)** offers opportunities to be assigned to other DHS components and outside agencies to gain cross-cutting experience and a DHS-wide perspective. Joint Duty Assignments are open to permanent, full-time employees at the GS-13 to GS-15 grade levels and can last up to a year. See the rolling list of openings and talk to your supervisor about ones that interest you.

The **Homeland Security Rotation Program (HSRP) and Virtual Homeland Security Rotation Program (VHSRP)** are sponsored by the DHS Office of the Chief Human Capital Officer and let you participate in cross-Component rotational assignments and government-wide joint rotational assignments. HSRP is a full-time commitment for three to six months, while VHSRP is project-based and can be done entirely virtual. You must be a permanent, full-time employee with at least one year of DHS experience and a "Proficient" or higher performance evaluation to be eligible. Approval from your supervisor is required. Learn more here.

If your department/agency has rotational/detail opportunities you wish to include, please email us at Education@cisa.dhs.gov.

Experience Opportunities

Mentoring

Mentoring is an excellent opportunity to hone your professional skillset, whether you're interested in being a mentor or a mentee. If you're a manager, consider becoming a mentor so that you can share your knowledge, insight, and best practices with more junior staff and refine your own leadership skills. If you're early in your career, consider becoming a mentee so you can receive one-on-one support and coaching to further your career. The government has a number of formal and informal mentoring programs, so talk to your manager about being paired up in a mentor-protégé relationship.

The **DHS Mentoring Program** is a nine-month program that pairs mentees with mentors from all disciplines. During the program, you'll create a Mentoring Action Plan, participate in meetings and developmental assignments, and get personalized support from your mentor. You should plan to commit at least two to four hours each month for mentoring activities, but the more you put in the more you'll get out. Employees at GS-14 grade level or below may apply to be a mentee online. Visit DHS Mentoring on Connect to get started.

If your department/agency has mentoring programs or opportunities you wish to include, please email us at Education@cisa.dhs.gov.

Experience Opportunities

Internships and Apprenticeships

Internships and apprenticeships are used for a wide range of placements in businesses, non-profit organizations and government agencies. Participants gain hands-on experience and on-the-job training you would otherwise not receive in a classroom setting. Internships and apprenticeships help you gain the skills and knowledge you need to succeed in the cybersecurity workforce. There are a variety of cybersecurity internships and apprenticeships across the federal government, so talk to your manager or supervisor about potential openings.

Internship Opportunities:

The CyberCorps®: Scholarship for Service (SFS) Program

The Pathways Internship Program

U.S. Intelligence Careers Student Programs
(includes cyber, digital forensics, computer science, and more)

Apprenticeship Opportunities:

Department of Labor's Apprenticeship Program

USAJobs

Department of Defense STEM Opportunities

If your department/agency has internship/apprenticeship programs or opportunities you wish to include, please email us at Education@cisa.dhs.gov.

Experience Opportunities

Self-study

Self-study is another tool you can use to sharpen your skills anytime and anywhere. Through self-study, you have the flexibility to pick topics that matter to you and study them at your own pace.

This virtual bookshelf offers a few suggestions to add to your reading list on cybersecurity, leadership, communication, and professional development. These materials are available at no-cost via download. Choose topics that match your interests, reflect on the information you learn, and discuss with your colleagues to enable continuous learning.

Tools & Templates

Cybersecurity Training Plan Worksheet

Discuss these questions with your supervisor and use the answers to select training and development activities to build your Cybersecurity Training Plan.

1. **What is my proficiency level for each target Work Role, Tasks & KSAs I want to improve?**

Work Roles	Proficiency Level

Tasks and KSAs	Proficiency Level

2. **What Work Roles, Tasks and KSAs do I want to target as a secondary priority?**

3. **What training and professional development activities should I take to improve my target Work Roles, Tasks, and KSAs?**

Tools & Templates

Sample Career Development Map

Do you need some ideas to get started in mapping out your Cybersecurity Training Plan? Below is a sample career development map to give you an idea of how to piece together different opportunities, from training courses to experience opportunities and more. You can tailor this map by swapping in any of the development activities throughout this Guide. The possibilities are endless! Talk to your manager for help in personalizing a development journey just for you and feed it into your Plan.

	Entry	Intermediate	Advanced
Professional Development Training & Certifications *What training and certifications should I consider?*	**Acquire Base Skills** • Consider general training courses to give you a well-rounded skillset, such as Network Security found on FedVTE • Research potential certifications of interest	**Hone Your Skills** • Consider more specialized training to hone your skillset • Get ready to take on more responsibilities by taking Cloud Security – What Leaders Need to Know • Take courses related to your desired certification	**Master Your Job** • Consider strategic & leadership training, such as ISACA Certified Information Security Manager Prep (CISM) • Become an expert in your area • Take exam to obtain certification
Stretch Opportunities *How can I "stretch" my capabilities into new areas?*	**Get Ready For Opportunity** • Communicate with your supervisor—be curious and ask questions • Join a special project team and practice collaboration and teamwork • Participate in meetings to take minutes and shadow more senior staff in action	**Seek Out Opportunity** • Lead a project • Consider a lateral detail or rotation • Join a professional organization	**Create Opportunity** • Serve in an "Acting" leadership role • Consider a vertical detail or rotation
Leadership Opportunities *How can I build my leadership skills as I move up the career ladder?*	**Lead Yourself** • Once basic skills are mastered, volunteer for additional responsibilities • Practice interpersonal, public speaking, and briefing skills • Find a mentor for one-on-on coaching	**Lead Teams** • Participate in the DHS Milestone Program • Become a mentor • "Give back" 12 hours of training and coaching	**Lead the Organization** • Hold a supervisory position and contribute to a mentorship program • Establish a Cybersecurity working group • Provide decision support and recommendations

Resources

CISA Resources

Looking for more information? Below is a list of additional programs, tools, and resources from across CISA that highlight cybersecurity education, training, and career development. From K-12 courses and scholarship opportunities to advanced cybersecurity training courses and career advancement, the below list has something for everyone! Check out the links below to learn more.

CISA Resources ◀ ▶ **Other Resources**

Title/Link	Description
CISA Careers	CISA is committed to hiring a highly talented, dedicated, diverse workforce and offers multiple opportunities for employment. Explore career options and join the CISA workforce.
Cyber Career Pathways Tool	The Cyber Career Pathways Tool presents a new and interactive way to explore work roles within the Workforce Framework for Cybersecurity (NICE Framework). It depicts the Cyber Workforce according to five distinct, yet complementary, skill communities.
CyberCorps®: Scholarship for Service (SFS) Program	The CyberCorps®: Scholarship for Service (SFS) Program is designed to recruit and train the next generation of cybersecurity professionals to meet the needs of federal and SLTT governments. CISA partners with the National Science Foundation (NSF) and the Office of Personnel Management (OPM) to provide institutions with funding towards scholarships for cybersecurity-related degree programs at two- and four-year colleges and universities.
Cybersecurity Publications Library	CISA's publications library is frequently updated with new resources and includes the latest cybersecurity topics and issues.
Cybersecurity Training & Exercises	Training is essential to preparing the cybersecurity workforce of tomorrow, and for keeping current cybersecurity workers up-to-date on skills and evolving threats. CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation.

Resources

CISA Resources

Looking for more information? Below is a list of additional programs, tools, and resources from across CISA that highlight cybersecurity education, training, and career development. From K-12 courses and scholarship opportunities to advanced cybersecurity training courses and career advancement, the below list has something for everyone! Check out the links below to learn more.

CISA Resources ◀ ▶ **Other Resources**

Title/Link	Description
FedVTE	The Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, U.S. military veterans and the public. Managed by CISA, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis.
National Centers of Academic Excellence in Cybersecurity (NCAE-C)	CISA and NSA jointly sponsor the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and expertise in cybersecurity.
National Cyber Awareness System	Five products in the National Cyber Awareness System offer a variety of information for users with varied technical expertise. Those with more technical interest can read the Alerts, Analysis Reports, Current Activity, or Bulletins. Users looking for more general-interest pieces can read the Tips.
National Initiative For Cybersecurity Careers and Studies (NICCS) website	NICCS has cybersecurity training/certification prep courses and education resources that connect government employees, students, educators, and industry with training providers throughout the nation.
NICE Framework Mapping Tool	The NICE Framework Mapping Tool takes the guesswork out of using the NICE Framework - simply answer questions about each cybersecurity related position and the tool will show you how each position aligns to the NICE Framework and what can be done to strengthen your cybersecurity team.

Resources

Other Resources

Looking for more information? Below is a list of additional programs, tools, and resources that highlight cybersecurity education, training, and career development. From K-12 courses and scholarship opportunities to advanced cybersecurity training courses and career advancement, the below list has something for everyone! Check out the links below to learn more.

CISA Resources	Other Resources

Title/Link	Description
CYBER.ORG	An online platform that works to ensure that every K-12 student gains foundational and technical cybersecurity knowledge and skills. This is accomplished by empowering teachers with the necessary resources and training to deliver cyber content to their students.
CyberCareers.gov	A platform for cybersecurity job seekers, federal hiring managers and supervisors, current federal cybersecurity employees, students and universities to have consolidated online access to tools, resources, and a guide to the cybersecurity workforce within the federal government.
Cybersecurity Capabilities Indicators	The Capability Indicators document lists recommended education, certification, training, experiential learning, and continuous learning that could signal an increased ability to perform a given NICE Framework Work Role.
Cybersecurity Executive Order Fact Sheet	A May 2021 Executive Order by President Biden to improve the nation's cybersecurity and protect federal government networks.
Cyberseek.org	An interactive jobs heat map and career pathway tool that shows cybersecurity jobs across the U.S. by state and metropolitan area. Jobs are organized by categories of the NICE Framework to which they align to.
DoD STEM Opportunities	Supports hands-on learning opportunities, teacher enrichment, scholarships, internships, and fellowships to inspire and cultivate a diverse pool of exceptional STEM talent.
DOL Apprenticeship Program	Apprenticeships help prepare individuals for the workforce by combining classroom instruction with hands-on training. The U.S. Department of Labor has various apprenticeship opportunities for employers and employees in the public and private sectors.

Resources

Other Resources

Looking for more information? Below is a list of additional programs, tools, and resources that highlight cybersecurity education, training, and career development. From K-12 courses and scholarship opportunities to advanced cybersecurity training courses and career advancement, the below list has something for everyone! Check out the links below to learn more.

CISA Resources	Other Resources
Title/Link	**Description**
FISSEA	An organization run by and for federal government information security professionals to assist federal agencies in strengthening their employee cybersecurity awareness and training programs. Their goal is to raise the general level of information security knowledge for the federal government and federally-related workforce.
(ISC)^2 Research	Gain a better understanding of cybersecurity employment trends, salary information, diversity and inclusion efforts, management and leadership issues, and the cybersecurity workforce as a whole by exploring the International Information System Security Certification Consortium (ISC)^2 research documents.
NIST Online Learning Content	Free and low-cost cybersecurity and information technology content and resources for career and professional development, educator training and curriculum, and K-12 education and games.
USAJobs	The U.S. federal government's official website for employment and internship opportunities.
Workforce Framework for Cybersecurity (NICE Framework)	Provides a set of building blocks for describing the Tasks, Knowledge, and Skills that are needed to perform cybersecurity work performed by individuals and teams. Through these building blocks, the NICE Framework enables organizations to develop their workforces to perform cybersecurity work, and it helps learners to explore cybersecurity work and to engage in appropriate learning activities to develop their knowledge and skills.

Resources

Contact Us

We would love to hear from you! As always, please contact us if you have any questions about the cybersecurity training, education, or career development opportunities mentioned in this Guide. We'd also love to get your feedback on additional cybersecurity training courses, tools, and resources to include in future updates as well as what we can do to improve this Guide. Please send inquiries to Education@cisa.dhs.gov – if we don't know we will direct your question to someone who does!

Cybersecurity Training

- Do you know of cybersecurity training that is available to the federal and/or SLTT workforce to include in our update?
- Are there any cybersecurity training topics you or your agency need that are not covered in this Guide?

Cyber Resources

- Did you find what you were looking for? Is our resource section complete? If not, send us the information you'd like us to potentially include in a future update of the Guide. Please remember that only government sources are published.

What Can We Do Better?

- It takes a cybersecurity village to determine what you do not know. What did we forget? How can we make this Guide more user-friendly?
- Did we cross every 't' and dot every 'i' – or did you find a typo or some other mistake? How embarrassing! Please let us know – we don't want anyone distracted by something silly.