CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION TECHNOLOGY

CYBERSECURITY & PRIVACY TRAINING CATALOG 2019

Spotlight | Specialty | Events

Provided by CMS Information Security & Privacy Group (ISPG)

01112019

Welcome to the Cybersecurity & Privacy Training Catalog!

Cybersecurity & Privacy Training & Awareness Program Mission: To deliver Security and Privacy awareness and training, and to identify and recommend aligned educational resources to benefit the CMS Community. Our engagement practices are dedicated to supporting a capable and engaged cyber workforce skilled and knowledgeable in the practices and processes necessary to protect our systems and enable the safe and authorized use of sensitive information.

I want to advance as a Cyber and Privacy professional.

Check out the Spotlight Track

I need the most current information to get my job done.

Participate in the Specialty Track

I want to collaborate with colleagues.

Join an in-person at an Event Track offering

I need to take role-based training.

Look for NICE course coding in catalog listings

I am an ISSO and want applicable training.

Look for ISSO Training Curriculum in the catalog

For technical support or special instructions regarding accessibility options and use of assistive technology, please send an email to CMSISPGTrainers@cms.hhs.gov for more information.

Let's Get Started!

How do I enroll in a classroom course?

If you are a federal government employee, please request training via the HHS Learning Portal. Specific registration links are provided within this catalog.

If you are a Contractor, please email your training request to CMSISPGTrainers@cms.hhs.gov. Please include your name, the class you would like to attend, and the contact information for your approving government supervisor.

How do I take an online course?

For webinars and live events enrollment instructions are provided in the CMS Broadcast email announcement. Follow the registration directions and links provided.

I have to take annual awareness training.

Visit CBT www.cms.gov/cbt

I have a question.

Email CMSISPGTrainers@cms.hhs.gov

2019 Training Planner

Spotlight Track

IT Risk Management	Control Families	Security and Privacy	POAMs and U
JAN - MAR	APR - JUN	JUL - SEP	OCT - DEC

Specialty Track

ISSO Forum

JAN 8	FEB 5	MAR 5
APR 9	MAY 7	JUN 4
JUL 2	AUG 6	SEP 10
OCT 8	NOV 5	DEC 4

all days 1:00 PM – 2:00 PM

CFACTS

FEB 19 – 20 9:00 AM – 4:00 PM, Online
MAY 14 – 15 9:00 AM – 4:00 PM, Classroom
AUG 20 – 21 9:00 AM – 4:00 PM, Online
NOV 12 – 13 9:00 AM – 4:00 PM, Classroom

Need to Know

Just-in-time training on hot topics each quarter. What you need to know when you need to know it. Delivered in a quick and easy to read format.

Event Track

Data Privacy Day	Winter Tech Exchange	Cybersecurity and Privacy Training Day	CISO Forum
FEB 5, CMS Auditorium	FEB 19, NIH Natcher Building	JUN 25, CMS Auditorium	OCT 22, CMS Auditorium

Click on a course *title* to learn more, or *date* to register (where available). All times are Eastern.

Prior supervisory approval is required to attend training. Course dates and times are subject to change.

ISSO Training Curriculum

This is a quick guide to catalog training offerings tailored to the Information System Security Officer (ISSO) community.

Training Tracks

Your First 90 Days

- **Navigating New Cybersecurity & Privacy Policies & Procedures** – Online
- **Working with CFACTS** – In Person or Online
- **ISSO Forum** – In Person or Online
- **How Hackers Hack and How to Protect Yourself** – Podcast

Security

- **All About the CMS Acceptable Risk Safeguards (ARS) 3.1** – Online
- **Cybersecurity Race** – Video
- **DevSecOps** – Quick Guide

Privacy

- **Your Role in Privacy at CMS** – Online
- **Incident Response at CMS** – Online
- **CMS Privacy Incident Response: Quick Guide for Business Owners** – Online

Click on a course *title* to learn more.

Legend

In Person | Online | Podcast | Quick Guide | Video

Spotlight Track

Introduction to Spotlight Track

Each Spotlight track topic is organized into a three-part learning series. A Spotlight topic will be introduced at the beginning of each quarter and will then be expanded upon to provide participants the opportunities to apply knowledge gained from prior learning opportunities. All Spotlight training is delivered via eLearning, so that participants can catch-up on a series or return to a specific lesson.

Spotlight Topic: IT Risk Management – Foundations (JAN – MAR)

Risk management helps to enable effective protections by accounting for potentially adverse circumstances or events. This Spotlight focuses on the basics of risk management including threats, vulnerabilities and impact. We will review risk management best practices. Learn about risk assessment policies and procedures for CMS IT systems.

Spotlight Topic: Your Role in Control Families (APR – JUN)

What's your role when it comes to security and privacy with control families? Deep dive into control families, core controls and control inheritance. Walk through control policy, standards and procedures. Learn about control standards.

Spotlight Topic: Security and Privacy (JUL – SEP)

Why security and privacy? How do we provide security and privacy in constantly changing environments? This Spotlight examines security and privacy and how they will continually shape CMS IT system operations.

Spotlight Topic: POAMs and U (OCT – DEC)

Take a closer look into Plan of Action and Milestones (POAM). Learn how this corrective action can effectively resolve an information security weakness. This Spotlight covers the POAM lifecycle from creation to close out.

Look for announcements and check-back for catalog updates as the above Spotlight training is rolled out across the year. See the following pages for currently available training opportunities.

Target Audience:

All CMS cyber and privacy professionals, including individuals with significant information security or privacy responsibilities: Business Owners (BOs), Information System Security Officers (ISSOs), Cyber Risk Advisors (CRAs), ISSO Contractor Support (ISSOCS) and IT Auditors.

Spotlight Series: DevSecOps

DevSecOps is the integration of information system security into development and operations. It provides continuous visibility into a system's security posture to prevent vulnerable applications from reaching production and delivers streamlined operations with simplified security reviews. This Spotlight introduces this methodology and enables participants to assess their system's readiness for DevSecOps.

Training	Description	Link
Quick Guide	Learn about the key components of DevSecOps at a glance.	Access Here
Video	This animated video explains DevSecOps and its benefits through a comparison to DevOps. Approximately 3 minutes.	Access Here
Check List	Is your system a candidate for DevSecOps? Use this checklist to assess your system's readiness.	Access Here

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND
Role ID (OPM Code)	722, 723, 731, 901	422, 441, 451, 461	212	311, 312, 331, 332, 333	111, 141,	611, 612, 622, 632, 651, 661	531

Note: The Role IDs listed above are helpful guides, the course may cover additional roles.

Spotlight Series: Your Role in Security

People are paramount to security and privacy protections at CMS. This Spotlight breaks the myth that cybersecurity is a technical issue. This Spotlight explains "social engineering" and other attacks which target personnel and the best methods to safeguard beneficiary data.

Training	Description	Link
Podcast*	How Hackers Hack and How to Protect Yourself. Approximately 13 minutes.	Access Here
Quick Guide	CMS Privacy Incident Response: Quick Guide for Business Owners.	Access Here
Quick Guide	The Role of the Reporter: Quick Guide for CMS personnel to learn when and how to report cybersecurity & privacy incidents.	Access Here

*NEW Podcast! Have you ever wondered about your part in helping to protect CMS systems and information? Listen to Pat Kast with the essentials on how to keep CMS safe and secure.

How Hackers Hack and How to Protect Yourself

Podcast: – runtime 13 minutes

"In today's podcast, we talk about How Hackers Hack and How to Protect Yourself. I'm your host, Pat Kast, and I'll be presenting three fascinating interviews, which delves into the devious minds of different types of hackers."

Pat Kast, Host of How Hackers Hack and How to Protect Yourself

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	PROTECT AND DEFEND
Role ID (OPM Code)	711, 712, 722, 723, 731, 732	421, 422, 411, 441	212	321	511, 521, 531, 541

Note: The Role IDs listed above are helpful guides, the course may cover additional roles.

Spotlight Series: Risk Management

Information systems, operations, technologies and threats are in constant motion. Risk management helps to enable effective protections by accounting for this continuous change. This Spotlight focuses on risk management as an operational model that can be applied in all CMS functions.

Training	Description	Link
Online	Risk Management: A Security Impact Analysis (SIA) Webinar - is an important risk management tool. In this workshop the current SIA process will be reviewed. Information systems, operations, technologies and threats are in constant motion. Risk management helps you enable effective protections by accounting for this continuous change. Approximately 35 minutes.	Access Here
Quick Guide	Security Impact Analysis (SIA) Quick Guide for Minor and Significant changes.	Access Here
Online	Risk Management: A Security Impact Analysis (SIA) Workshop - This webinar on Configuration Management and Security Impact Analysis, builds on the recent SIA workshop. This webinar will broaden the discussion and provide additional context for the SIA process. Topics covered will include the relationship between guidance and implementation, the CMS policy hierarchy, the SIA process within CM and methods to evaluate a change as minor or significant. Approximately 30 minutes.	Access Here

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND
Role ID (OPM Code)	722, 723,	421, 422, 431, 441, 451, 461	332	121	611, 651, 652	511, 521, 531, 541

Note: The Role IDs listed above are helpful guides, the course may cover additional roles.

Spotlight Series: Navigating New Cybersecurity & Privacy Policies & Procedures
Learn about the CMS policy framework and how to best use these documents in cybersecurity planning and operations. Also learn revisions to the Information System Security and Privacy Policy (IS2P2), Acceptable Risk Safeguards (ARS) and Risk Management Handbooks (RMH).

Training	Description	Link
Quick Guide	Looking for a policy quick guide? At-a-glance, learn how to find what you need by navigating the cybersecurity policy, standards, and procedures.	Access Here
Video	Cyber Race - Quick, fun video, to see the policy framework in action. Approximately 3 minutes.	Access Here
Online	Navigating New Policies & Procedures - Listen to the experts explain the CMS cybersecurity and privacy policy hierarchy, hear policy use case examples, and learn about recent and upcoming changes to the CMS policy framework. Approximately 45 minutes.	Access Here

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND
Role ID (OPM Code)	711, 712, 722, 723, 731, 732, 751, 752, 804	411, 421, 422, 431, 441, 451, 461	211, 212, 221	311, 312, 331, 332, 333, 321	111, 112, 121, 131, 132, 141, 151	611, 612, 631, 632, 641, 651, 652, 666, 671	511, 521, 531, 541

Note: The Role IDs listed above are helpful guides, the course may cover additional roles.

Specialty Track

Introduction to Specialty Track

The Specialty track is focused on various training topics that are timely and tailored to participant roles. Track offerings range from information exchange forums to specialized topic training to deep dive skills-based learning. Many Specialty track offerings are available in eLearning formats for anytime on-demand access.

ISSO Forum

Collaborate with other cybersecurity and privacy colleagues supporting CMS systems to address current topics. Join the forum and gain guidance on wide-ranging security challenges that impact our business. Each forum includes an open question and answer session where topics can be raised to help determine solutions.

Target Audience: CMS cybersecurity professionals, Information System Security Officers (ISSOs), Cyber Risk Advisors (CRAs), ISSO Contractor Support (ISSOCS)

Schedule Information:

Date	Time	Location	Participate*
JAN 8	1:00 PM – 2:00 PM	Room C-114 and Online	See ISSO Email
Feb 5	1:00 PM – 2:00 PM	Room C-111 and Online	See ISSO Email
MAR 5	1:00 PM – 2:00 PM	Room C-111 and Online	See ISSO Email
APR 9	1:00 PM – 2:00 PM	Room C-111 and Online	See ISSO Email
MAY 7	1:00 PM – 2:00 PM	Room C-111 and Online	See ISSO Email
JUN 4	1:00 PM – 2:00 PM	Room C-111 and Online	See ISSO Email
JUL 2	1:00 PM – 2:00 PM	Room C-111 and Online	See ISSO Email
AUG 6	1:00 PM – 2:00 PM	Room C-110 and Online	See ISSO Email
SEP 10	1:00 PM – 2:00 PM	Room C-110 and Online	See ISSO Email
OCT 8	1:00 PM – 2:00 PM	Room C-110 and Online	See ISSO Email
NOV 5	1:00 PM – 2:00 PM	Room C-110 and Online	See ISSO Email
DEC 4	1:00 PM – 2:00 PM	Room C-114 and Online	See ISSO Email

* Registration information is provided monthly via ISSO email Distribution List (DL).

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND

Note: Role ID 722 is regularly covered, forum topics/discussion may address additional roles.

Working with CFACTS

This hands-on two-day course is designed to train new users to properly use CFACTS, a web-based system tool, used for collecting the security and privacy management data required by the Federal Information Security Management Act (FISMA) systems. This tool stores and organizes information essential to your system's secure operation. Common tasks covered in class include: system lifecycle support, security assessment remediation using Plan of Action Milestones (POA&M), analysis gained through the Privacy Impact Assessments (PIA) tool, as well as the creation of Authorization to Operate (ATO) packages. Key course lessons include: tool navigation, what, where, and when to enter your system's information, and tips for completing common security and privacy documentation.

Target Audience: New users to CFACTS including Business Owners (BOs), Information System Security Officers (ISSOs), ISSO Contractor Support (ISSOCS), and anyone else working with CFACTS.

Schedule Information:

Date	Time	Location	Federal Employee Participation*
FEB 19 - 20	9:00 AM – 4:00 PM	Online	Register Here
MAY 14 - 15	9:00 AM – 4:00 PM	CMS Training Center (7111 Security Blvd)	Register Here
AUG 20 - 21	9:00 AM – 4:00 PM	Online	Register Here
NOV 12 - 13	9:00 AM – 4:00 PM	CMS Training Center (7111 Security Blvd)	Register Here

***Contractor Participation**: to register send email to* CMSISPGTrainers@cms.hhs.gov. *Please include your name, the class you would like to attend, and your approving COR, GTL or ISSO contact information.*

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND
Role ID (OPM Code)	711, 712, 722, 723, 731, 732, 751, 752, 804	421, 422, 431, 411, 441, 451, 461	211, 212, 221	311, 312, 321, 331, 332, 333	121, 111, 112, 131, 132, 141, 151	611, 612, 631, 632, 641, 651, 652, 666, 671	511, 521, 531, 541

Note: The Role IDs listed above are helpful guides, the course may cover additional roles.

Need to Know

The Need to Know training series provides just in time training, on a variety of current topics, when it is needed. Need to Know training is relevant learning customized for busy CMS personnel that is easy to understand and delivered in an online quick read format.

Target Audience: Need to Know audiences varies by training topic. The target audience is identified with each Need to Know training offering.

Need to Know Training: Quick Guides:

Training	Description	Link
Quick Guide	Role-based training for CMS Cybersecurity and Privacy	Access Here
Quick Guide	Security Impact Analysis (SIA)	Access Here
Quick Guide	System Interconnections	Access Here
Quick Guide	CMS Cybersecurity is Lookin' NICE	Access Here

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND
Role ID (OPM Code)	711, 712, 722, 723, 731, 732, 751, 752, 804	421, 422, 431, 411, 441, 451, 461	211, 212	311, 312, 321, 333	112, 121, 131, 132, 141, 151	611, 612, 631, 632, 641, 651, 652, 666, 671	511, 521, 531, 541

Note: The Role IDs listed above are helpful guides, the course may cover additional roles.

All about CMS Acceptable Risk Safeguards (ARS) 3.1

This webinar provides additional clarification on the ARS which was released January 31, 2017. Learn how the mandatory baseline controls align with NIST and how controls can be implemented to achieve cost-effective, risk-based security that supports organizational mission and business requirements. A case study by Medicare Administrative Contractors (MACs) will be provided on how a defined set of controls have been incorporated into a mandatory baseline to meet their specific requirements.

Target Audience: This webinar is designed to provide useful information to ISSOs, Business Owners, System Owners and other stakeholders in implementing the CMS ARS requirements.

Date	Time	Location	Participate
Previously Recorded on 12/12/2017	Approximately 1 hour	On Demand	Access Here

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND
Role ID (OPM Code)	711, 712, 722, 804	441, 451, 461	121, 111, 112, 131, 132, 141, 151	611, 612, 631, 632, 641, 651, 652, 666, 671	511, 521, 541

Note: The Role IDs listed above are helpful guides, the course may cover additional roles.

Your Role in Privacy at CMS

Privacy and Security go hand in hand and are integrated into a single comprehensive program at CMS. This webinar introduces you to Federal cybersecurity requirements, important laws and policies dealing with privacy, and addresses our daily responsibilities at CMS. The webinar highlights the Fair Information Practice Principles (FIPS), along with discussing the circumstances surrounding privacy breaches. Guidance for handling privacy data, privacy concerns, and privacy incidents will also be discussed.

Target Audience: All CMS cyber and privacy professionals including Business Owners (BOs), Information System Security Officers (ISSOs), Cyber Risk Advisors (CRAs), and ISSO Contractor Support (ISSOCS).

Date	Time	Location	Participate
Previously Recorded on 09/27/2017	Approximately 1 hour	On Demand	Access Here

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND
Role ID (OPM Code)	711, 712, 722, 732, 751, 752	411,421, 422, 431, 441, 451, 461	221	311, 312, 321, 331, 332, 333	511, 521, 531, 541	611, 612, 631, 632, 641, 651, 652, 666, 671	111, 112, 121

Note: The Role IDs listed above are helpful guides, the course may cover additional roles.

Incident Response at CMS

This course covers the requirements and processes that support cybersecurity and privacy incident response handling and reporting. Participants will learn about the Incident Management Team (IMT) and part of the CMS Cybersecurity Integration Center (CCIC). They will also learn the direction and support provided by CCIC to all CMS components and contractors conducting corrective actions mitigating security and privacy incidents.

Target Audience: All CMS cyber and privacy professionals including Business Owners (BOs), Information System Security Officers (ISSOs), Cyber Risk Advisors (CRAs), and ISSO Contractor Support (ISSOCS).

Date	Time	Location	Participate
Previously Recorded on 08/23/2017	Approx. 1 hour	On Demand	Access Here

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND
Role ID (OPM Code)	711, 712, 722, 804	441, 451, 461	211, 212, 221	111, 112, 121, 131, 132, 141, 151	611, 612, 631, 632, 641, 651, 652, 666, 671	511, 521, 541

Note: The Role IDs listed above are helpful guides, the course may cover additional roles.

Event Track

Introduction to Event Track

ISPG develops and curates a variety of industry leading events throughout the year. Check the Event Track periodically for opportunities to gain knowledge and skills that are essential for various roles at CMS. Join with your colleagues in exploring ideas and new solutions. Offerings include an unparalleled combination of education along with training on technologies and trends. They also provide the opportunity for participants to extend their professional networks by building new connections with like-minded colleagues.

Data Privacy Day

The event will raise awareness and promote privacy education. There will be breakout sessions and panel discussions. Privacy compliance, privacy laws and regulations will be discussed.

Privacy Day serves to foster communication among stakeholders interested in advancing data protection and privacy.

Target Audience: All CMS cyber and privacy professionals including any employees with significant security or privacy responsibilities.

Schedule Information:

Date	Time	Location	Participate
FEB 5	9:00 AM – 12:30 PM	CMS Auditorium	See CMS Broadcast

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND

Note: Role IDs 731, 732, 722 are covered, discussion may address additional roles.

HHS Winter 2019 Tech Exchange

The Security Design and Innovation team is hosting another Technology Exchange! This Virtual Tech Exchange is an opportunity for HHS stakeholders to share lessons learned from various technology implementations and security platforms from federal employees and cutting-edge vendors.

Target Audience: All CMS cyber and privacy professionals including any employees with significant security or privacy responsibilities.

Schedule Information:

Date	Time	Location	Participate
FEB 19	9:00 AM – 4:00 PM	NIH Natcher Building	Techexchange@HHS.gov

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND

Note: Role ID (OPM Code) -- This event has multiple sessions. To meet role-based training requirements, review session descriptions and select those that align with your role.

CMS Cybersecurity & Data Privacy Training Day

The CMS Cybersecurity & Data Privacy Day will be hosted by the Information Security Privacy Group (ISPG) at CMS. The Vision for ISPG is to provide leadership to CMS in managing information security and privacy risks appropriate for evolving cyber threats. The Mission is to enable the safe use of sensitive and privacy data while servicing the healthcare needs of the nation.

This event will include 6 Breakout Sessions as well as a Keynote which will consist of content geared towards all CMS Cyber Professionals as well as any employees with significant security and privacy responsibilities. Table top displays from prime contractors and small businesses will be a highlight for information exchange and networking.

Target Audience: All CMS cyber and privacy professionals including any employees with significant security or privacy responsibilities.

Schedule Information:

Date	Time	Location	Participate
JUN 25	9:00 AM – 3:00 PM	CMS Auditorium	See CMS Broadcast

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND

Note: Role ID (OPM Code) -- This event has multiple sessions. To meet role-based training requirements, review session descriptions and select those that align with your role.

CMS CISO Cybersecurity Awareness & Training Forum

In support of National Cybersecurity Awareness Month, please join the CMS Chief Information Security Officer at our Annual Cybersecurity Awareness & Training Forum. Creating a culture of cybersecurity is critical for all organizations, including CMS. The internet is now pervasive in our day-to-day activities and along with that comes the ever-increasing risk of cyber-attacks that can result in harm to those affected.

Knowing how to identify and prevent common cyber-attacks helps promote cybersecurity for everyone. The goal of National Cybersecurity Awareness month is to engage and educate CMS staff on protecting information technology systems and data from cyber-attacks and to promote clear and consistent communications about cybersecurity and privacy protections.

Target Audience: All CMS cyber and privacy professionals including any employees with significant security or privacy responsibilities.

Schedule Information:

Date	Time	Location	Participate
OCT 22	9:00 AM – 2:00 PM	CMS Auditorium	See CMS Broadcast

NICE Role-Based Categories:

Category	OVERSEE AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURELY PROVISION	PROTECT AND DEFEND

Note: Role ID (OPM Code) -- This event has multiple sessions. To meet role-based training requirements, review session descriptions and select those that align with your role.

Additional Training Opportunities

Provider	Description
CMS ISPG Beneficiary Data Protection Initiative (BDPI) http://intranet.cms.gov/Component/OEI/ISPG/Beneficiary-Data-Protection-Initiative.html	The Beneficiary Data Protection Initiative mission is to protect the personal information of CMS employees and the millions of people we serve. Learn about BDPI "Phishing" campaigns, Non-Malicious emails and more.
Fed VTE **Federal Virtual Training Environment** https://fedvte.usalearning.gov/	Provides a free online, on-demand cybersecurity training system. Individuals with a .gov or .mil email address can register and use the system.
HHS LMS **Health and Human Services Learning Management System** http://intranet.cms.gov/Component/OOM/DTD/Learning-Portal.html	Provides over 3000 Skill Soft courses, including cybersecurity certification preparatory training and continuing education unit (CEUs), and Books 24/7
IASE **INFORMATION ASSURANCE SUPPORT ENVIRONNENT (I)** https://iase.disa.mil/Pages/index.aspx	Provides cybersecurity information, policy, guidance and training for cybersecurity professionals. Some portions of the site are also available to the Federal Government and the public.
SANS https://www.sans.org/	Provides a source for information security training and security certification. SANS training can be taken in a classroom setting from SANS-certified instructors, self-paced over the Internet, or in mentored settings in cities.
SPLUNK https://www.splunk.com/en_us/training.html	Provides training on Splunk technology used to search, analyze, and visualize the machine-generated data gathered from websites, applications, sensors, and devices. Splunk is also used for application management, security and compliance, as well as business and Web analytics.

Please note: CMS ISPG does not promote or endorse any vendor. The vendors listed are provided only as examples. Government offerings may only be available to federal employees.

Appendix: NICE Framework

Introduction to NICE Appendix

CMS is committed to the development of a strengthened cybersecurity workforce. ISPG offers role-based training opportunities mapped to the National Initiative for Cybersecurity Education (NICE) framework.

Many training opportunities listed in this catalog include the NICE role-based categorization to help identify the training you need. The tables on the following pages provide a summary of NICE categories and roles.

Detailed information on the NICE framework can be found at NIST.

NICE Category: Securely Provision (SP)

NICE Specialty Area	Work Role	Work Role Definition	Role ID
Risk Management (RSK)	Authorizing Official/Designating Representative	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).	611
	Security Control Assessor	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).	612
Software Development (DEV)	Software Developer	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.	621
	Secure Software Assessor	Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.	622
Systems Architecture (ARC)	Enterprise Architect	Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.	651
	Security Architect	Ensures that the stakeholder security requirements necessary to protect the organization's mission and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting systems supporting those missions and business processes.	652
Technology R&D (TRD)	Research & Development Specialist	Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.	661
Systems Requirements Planning (SRP)	Systems Requirements Planner	Consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.	641
Test and Evaluation (TST)	System Testing and Evaluation Specialist	Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.	671
Systems Development (SYS)	Information Systems Security Developer	Designs, develops, tests, and evaluates information system security throughout the systems development life cycle.	631
	Systems Developer	Designs, develops, tests, and evaluates information systems throughout the systems development life cycle.	632

NICE Category: Operate and Maintain (OM)

NICE Specialty Area	Work Role	Work Role Definition	Role ID
Data Administration (DTA)	Database Administrator	Administers databases and/or data management systems that allow for the secure storage, query, protection, and utilization of data.	421
	Data Analyst	Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.	422
Knowledge Management (KMG)	Knowledge Manager	Responsible for the management and administration of processes and tools that enable the organization to identify, document, and access intellectual capital and information content.	431
Customer Service and Technical Support (STS)	Technical Support Specialist	Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).	411
Network Services (NET)	Network Operations Specialist	Plans, implements, and operates network services/systems, to include hardware and virtual environments.	441
Systems Administration (ADM)	System Administrator	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).	451
Systems Analysis (ANA)	Systems Security Analyst	Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.	461

NICE Category: Oversee and Govern (OV)

NICE Specialty Area	Work Role	Work Role Definition	Role ID
Legal Advice and Advocacy (LGA)	Cyber Legal Advisor	Provides legal advice and recommendations on relevant topics related to cyber law.	731
	Privacy Officer/Privacy Compliance Manager	Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams.	732
Training, Education, and Awareness (TEA)	Cyber Instructional Curriculum Developer	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.	711
	Cyber Instructor	Develops and conducts training or education of personnel within cyber domain.	712
Cybersecurity Management (MGT)	Information Systems Security Manager	Responsible for the cybersecurity of a program, organization, system, or enclave.	722
	Communications Security (COMSEC) Manager	Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).	723
Strategic Planning and Policy (SPP)	Cyber Workforce Developer and Manager	Develops cyberspace workforce plans, strategies, and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.	751
	Cyber Policy and Strategy Planner	Develops and maintains cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.	752
Executive Cyber Leadership (EXL)	Executive Cyber Leadership	Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.	901
Program/Project Management (PMA) and Acquisition	Program Manager	Leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with agency or enterprise priorities.	801
	IT Project Manager	Directly manages information technology projects.	802
	Product Support Manager	Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.	803
	IT Investment/Portfolio Manager	Manages a portfolio of IT investments that align with the overall needs of mission and enterprise priorities.	804
	IT Program Auditor	Conducts evaluations of an IT program or its individual components to determine compliance with published standards.	805

NICE Category: Protect and Defend (PR)

NICE Specialty Area	Work Role	Work Role Definition	Role ID
Cybersecurity Defense Analysis (CDA)	Cyber Defense Analyst	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.	511
Cybersecurity Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.	521
Incident Response (CIR)	Cyber Defense Incident Responder	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.	531
Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.	541

NICE Category: Analyze (AN)

NICE Specialty Area	Work Role	Work Role Definition	Role ID
Threat Analysis (TWA)	Threat/Warning Analyst	Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.	141
Exploitation Analysis (EXP)	Exploitation Analyst	Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.	121
All-Source Analysis (ASA)	All-Source Analyst	Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.	111
	Mission Assessment Specialist	Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.	112
Targets (TGT)	Target Developer	Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.	131
	Target Network Analyst	Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.	132
Language Analysis (LNG)	Multi-Disciplined Language Analyst	Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates and maintains language-specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.	151

NICE Category: Collect and Maintain (CO)

NICE Specialty Area	Work Role	Work Role Definition	Role ID
Collection Operations (CLO)	All Source-Collection Manager	Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.	311
	All Source-Collection Requirements Manager	Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.	312
Cyber Operational Planning (OPL)	Cyber Intel Planner	Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.	331
	Cyber Ops Planner	Develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.	332
	Partner Integration Planner	Works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.	333
Cyber Operations (OPS)	Cyber Operator	Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executes on-net operations.	321

NICE Category: Investigate

NICE Specialty Area	Work Role	Work Role Definition	Role ID
Cyber Investigation (INV)	Cyber Crime Investigator	Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.	221
Digital Forensics (FOR)	Law Enforcement /CounterIntelligence Forensics Analyst	Conducts detailed investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.	211
	Cyber Defense Forensics Analyst	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.	212