CMS CYBERSECURITY AND PRIVACY TRAINING

CATALOG 2023

Provided By:
CMS Office of Information Technology (OIT) and
Information Security and Privacy Group (ISPG)

JANUARY 2023

Table of Contents

Cybersecurity & Privacy Training Roles 3

Let’s Get Started 4

Online Live Events 5

Ask a CISO 6

Significant Cybersecurity and Privacy Roles 7

CMS Cybersecurity Community Forum 8

CFACTS 9

Need to Know 10

Contingency Planning 11

Incident Response at CMS 12

Your Role in Privacy at CMS 13

Your Role in Security 14

DevSecOps 15

Risk Management - Foundations 16

Phishing at CMS 17

Phishing – Did you know? 18

Cyber Training Videos 19

Podcast 20

ISSO Cybersecurity Knowledge Assessment 21

ISSO Score Card 22

Additional Training Opportunities 23

NICE Appendix 24

Everyone Plays a Role on the Cybersecurity and Privacy Team

Here at CMS, everyone in the CMS community -- all employees, managers and contractors -- plays a vital role by building a workforce that enhances national security and promotes economic prosperity. If everyone does their part – implementing stronger cybersecurity practices, raising community awareness and education – our interconnected world will be safer and more resilient for everyone.

Every year, we take the Information System Security and Privacy Awareness (ISSPA) course. The ISSPA course is mandatory for all users of CMS Information Systems when users are issued a CMS User ID. It is also mandatory for users to retake the Information Systems Security and Privacy Awareness course annually in conjunction with the mandatory annual certification of CMS User IDs.

For your convenience this year, completions of the Information Systems Security and Privacy Awareness course completes role-based training by completing the integrated Risk Management role-based training module.

Click here for CMS Information Systems Security and Privacy Awareness (ISSPA) training.

Cybersecurity & Privacy

JANUARY 2023

E **Everyone**

Look for the "E" next to courses that are applicable to everyone at CMS.

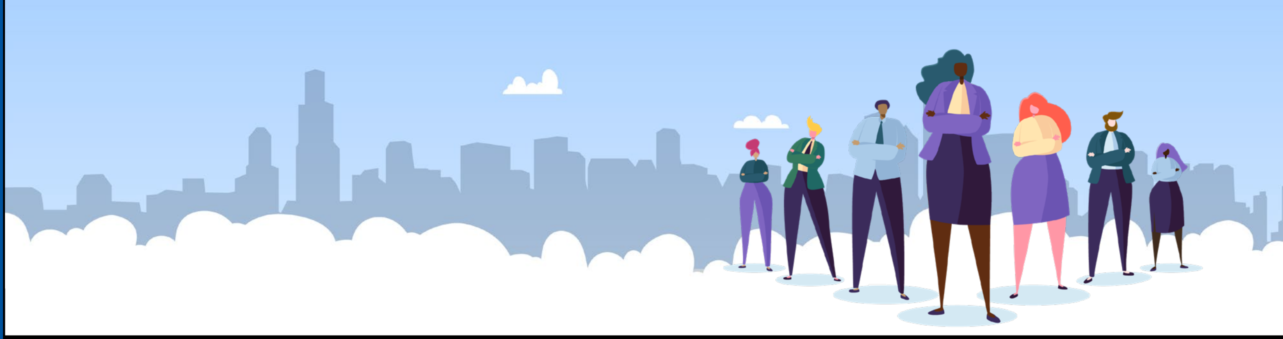
X **Cybersecurity Explorer**

For those new to cybersecurity or just interested in cybersecurity topics.

C **Cybersecurity Workforce Community**

For those currently practicing cybersecurity and all Information System Security Officers (ISSO).

Look for the symbols through the catalog that will map to your training.



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 can 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 a question. Who do I send it to?

Email CMSISPGTrainers@cms.hhs.gov.

I need technical Support.

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.

What is the CMS Cybersecurity & Privacy Awareness & Training program mission?

The program's mission is 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.

Online Live Events

CMS Cybersecurity CISO Forum – April 20th, 2023

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.

CMS CyberWorks – October 2023

Cybersecurity is challenging in a world where technologies are always improving and determined hackers are an evolving threat. We must continue to be vigilant by protecting CMS' systems and valuable data.

Cybersecurity and privacy professionals from both government and the private sector will discuss cybersecurity and privacy priorities, trends, and improvements and ways to confront unparalleled security challenges:

- Privacy
- Cybersecurity
- Risk

Target Audience: Entire CMS workforce, including any employees with significant security or privacy responsibilities.

Ask a CISO

E

Monthly
Please join us for our scheduled "Ask a CISO." You will get insider security tips, be able to ask questions and get insights on the newest trends in cybersecurity. The CISOs are here to help you improve your cyber knowledge, give you a better understanding of the services that ISPG offers, and help you understand how Cybersecurity works here at CMS.

Target Audience: All CMS workforce, including any employees with significant security or privacy responsibilities.

***See CMS Notification for participation**

Significant Cybersecurity and Privacy Roles

All the courses are aligned to the specialty areas of The Workforce Framework for Cybersecurity National Initiative for Cybersecurity Education (NICE).

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 CMS positions. It also provides a common lexicon that is used to develop cybersecurity curricula that better prepares students for current and future cybersecurity workforce needs.

Look for NICE course color coding in the catalog next to the course listings.

CMS Cybersecurity Community (C3) 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: Anyone interested in knowing more about cybersecurity at CMS to include CMS cybersecurity professionals, Information System Security Officers (ISSOs), Cyber Risk Advisors (CRAs), ISSO Contractor Support (ISSOCS).

SCHEDULE INFORMATION:

Date	Time	Location	Participate*
JAN 3	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
FEB 7	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
MAR 14	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
APR 4	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
MAY 2	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
JUN 6	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
JUL 11	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
AUG 1	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
SEP 5	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
OCT 3	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
NOV 7	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email
DEC 5	1:00 PM – 2:00 PM	Zoom	See CMS Broadcast Email

* Registration information is provided monthly via CMS Broadcast email.

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, 321, 331, 332, 333	111,121, 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.

CFACTS

Working with CFACTS – Introduction to Risk Management & Risk Management Framework (RMF)

This is a two-day course designed to train new users on the NIST RISK Management Framework (RMF) and how the CMS FISMA Continuous Tracking System (CFACTS) maps to the RMF steps. The CFACTS tool stores and organizes information essential to your system's secure operation. Common tasks covered in class include:

- RMF Steps
- Roles and responsibilities
- Security assessment remediation Plan of Action Milestones
- Privacy Impact Assessments (PIA)
- Information Security Risk Assessment (ISRA)
- Authorization to Operate (ATO) packages to request for certification of the FISMA system.

Key course lessons include tool navigation of CFACTS; what, where, and when to enter your system's information; and tips for completing common security and privacy documentation. Target Audience: New users who need to understand the NIST RMF and how to use the CMS GRC tool CFACTS to create the Authorization Package(s) and perform the data entry, Cyber Risk Advisors (CRAs), Information System Security Officers (ISSOs), and ISSO Contractor Support (ISSOCs). But any new user or stakeholder is invited to also include; Business Owners (BOs), security contractor support staff or anyone else working with the NIST RMF and CFACTS tool are welcome.

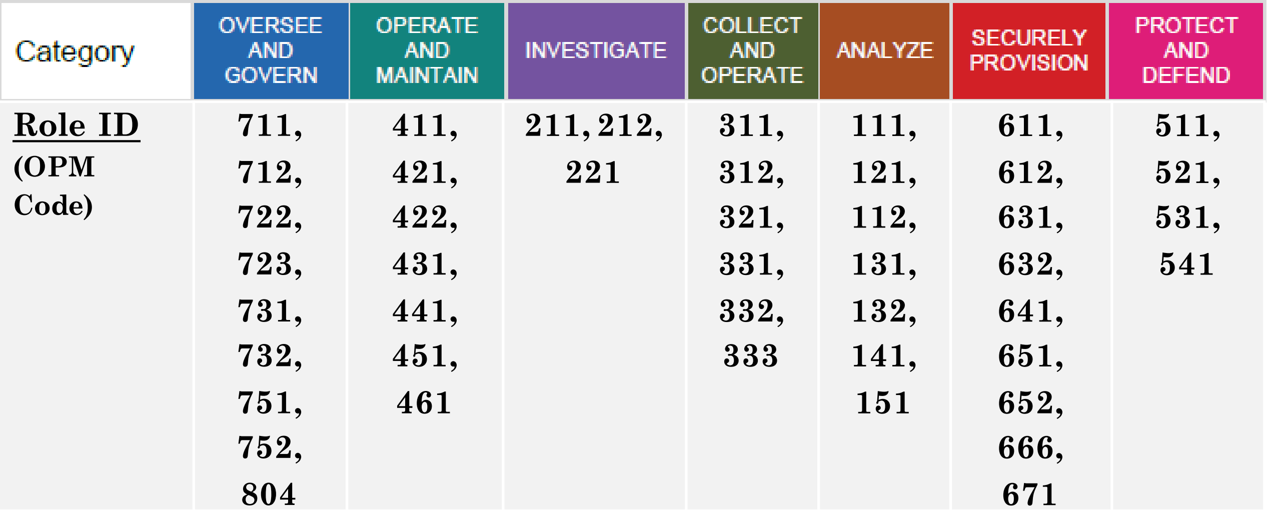
SCHEDULE INFORMATION:

*Schedule is subject to change

Date	Time	Location	Federal Participate*
JAN 24-25	9:00 AM – 4:00 PM	Zoom	Register Here
MAY 9-10	9:00 AM – 4:00 PM	Zoom	Register Here
JULY 11-12	9:00 AM – 4:00 PM	Zoom	Register Here
SEP 12-13	9:00 PM – 4:00 PM	Zoom	Register Here
NOV 14-16	9:00 AM – 4:00 PM	Zoom	Register Here
NOV 14-15	9:00 AM – 4:00 PM	Zoom	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	411, 421, 422, 431, 441, 451, 461	211, 212, 221	311, 312, 321, 331, 332, 333	111, 121, 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 vary 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	Your Role-Based Training – CMS Contractors	Access Here
Quick Guide	System Interconnections	Access Here
Quick Guide	Security Impact Analysis (SIA)	Access Here
Quick Guide	Role-Based Training for CMS Cybersecurity & Privacy	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	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.

Contingency Planning

E C

This training is an introductory course on contingency planning focusing on Continuity of Operations Plans (COOP), Business Impact Analysis (BIA), Disaster Recovery Plans (DRP), and Information System Contingency Plans (ISCP).

Target Audience: Individuals with significant information security and privacy roles and responsibilities are required to complete Role-Based Training (RBT).

Training	Time	Location	Participate
Online	Approximately 10 min	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, 723, 731, 732, 751, 752, 801, 802, 803, 804, 805, 901						511, 521, 531, 541

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

Incident Response at CMS

This Incident Response at CMS webinar 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.

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

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).

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, 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	711, 712, 722, 804

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.

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

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).

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

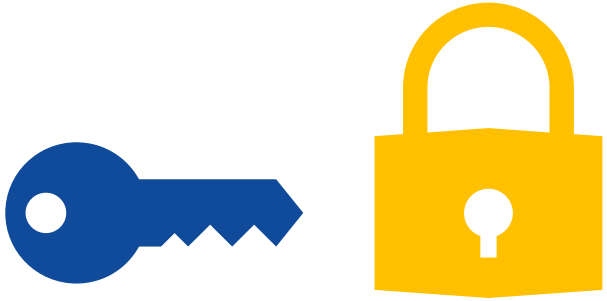
Note: The Role IDs listed above are helpful guides; the course may cover additional roles.

Your Role in Security

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

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.

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



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	411, 421, 422, 441	212	321	511, 521, 531, 541	711, 712, 722, 723, 731, 732	411, 421, 422, 441

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

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.

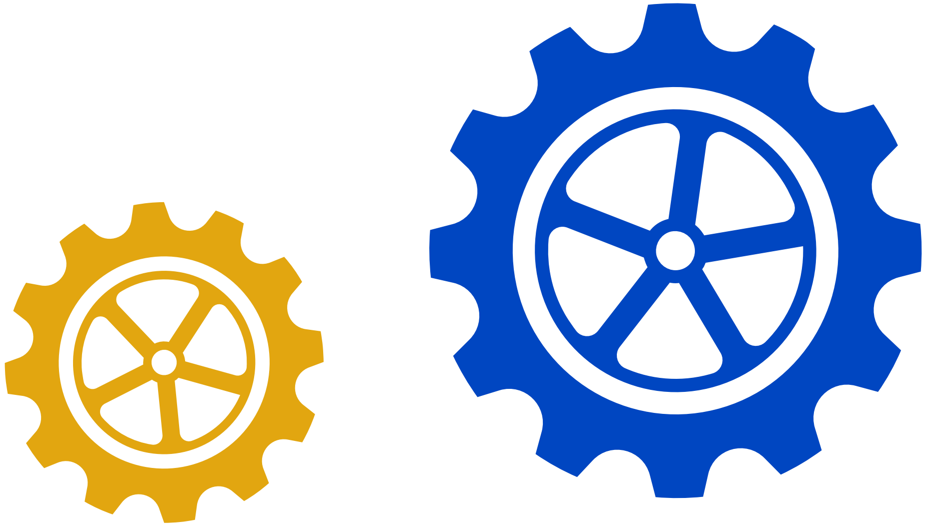
Target Audience: All CMS cyber and privacy professionals, including individuals with significant information security or privacy responsibilities: Business Owners (BOs), Information System Security Officers (ISSOs), Cyber Risk Advisors (CRAs), ISSO Contractor Support (ISSOCS) and IT Auditors.

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.



Risk Management – Foundations

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

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.

Training	Description	Link
Video	Watch this fun video and learn about the foundations of risk management, including threat, impact, likelihood and vulnerabilities. Approximately 5 minutes.	Access Here
Case Study	Read about risk management foundations when it comes to conducting patch management risk assessments.	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	421, 422, 431, 441, 451, 461	332	121	611, 651, 652	511, 521, 531, 541	722, 723

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

Phishing at CMS

E

One of the greatest cybersecurity risks to CMS are “phishing” attacks. The term phishing describes email that appears to be trustworthy but is fraudulent, designed to compromise CMS information and systems.

To reduce this critical risk, OIT/ISPG is providing specialized training. Focused on strengthening CMS cybersecurity, the training will cover phishing risks, techniques to detect phishing emails, and methods to avoid and/or report suspicious emails.

Target Audience: All CMS personnel with a CMS email account.

Training	Time	Location	Participate
Online	Approximately 4 min	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, 723, 731, 732, 751, 752, 801, 802, 803, 804, 805, 901						511, 521, 531, 541

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

Phishing

Did you know?

Did you know phishing scams can target a single person, an operational unit or the entire agency? Phishing (pronounced "fishing") is a type of social engineering that uses various methods to entice unsuspecting victims to “take the bait,” much like a real fish would do. Phishing scams come in many variations and target everyone – even us! Did you know phishing can look like legitimate accounts and websites? Phishing uses deceptive narratives, such as websites that look real but aren’t, emails that falsely alert users of a problem with their account, and messages that provide fake links. To learn more, click the links below.

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.

Training	Description	Link
Quick Guide	Learn about Phishing - Did you know? Phishing scams can be hiding in plain sight.	Access Here
Quick Guide	This quick guide explains how Phishing scams come in many variations.	Access Here
Quick Guide	Use this quick guide to learn more about Phishing scams that go beyond email.	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, 321, 331, 332, 333	111, 112, 131,132, 133, 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.

Cyber Training Videos

Adaptive Capabilities Testing

Duration: 3.35 minutes

Privacy Impact Assessment

Duration: 3.56 minutes

Security Impact Analysis

Duration: 5.09 minutes

Privacy Act System of Records Notice

Duration: 3.35 minutes

Plan of Action and Milestones

Duration: 5.08 minutes

The Audit

Duration: 8.03 minutes

Data Guardian

Duration: 4.01 minutes

Data Sharing Agreements

Duration: 3.37 minutes

Visit the Video Channel with Cybersecurity and Privacy Training Videos provide informative entertaining training on a variety of current topics. This growing catalog of educational cyber training videos allows you to pick topics that are important to you. All are mapped to NICE roles.

NOTE: Additional videos are added throughout the year.

Podcast

Hackers Hack and How to Protect Yourself – 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 delve into the devious minds of different types of hackers."

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	411, 421, 422, 441	212	321	511, 521, 531, 541

Risk Management – runtime 5 minutes

Managing risk pertains to everyone at CMS regardless of your role. This podcast aims to help everyone at CMS to better understand and effectively manage risk to mitigate any potential harm and negative impacts to day-to-day operations.

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	411, 421, 422, 431, 441. 451	212	321	511, 521, 531, 541

The Audit Podcast – runtime 8 minutes

Who says learning about audits must be boring?

The goal is to demystify the audit process and let listeners know that audits improve our cybersecurity – they don't just make more work.

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, 732, 752, 805	411, 421, 441, 451, 461	211, 212, 221	311, 312, 321, 331, 332, 333	111	611, 612, 641, 651, 652, 671	511, 541

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

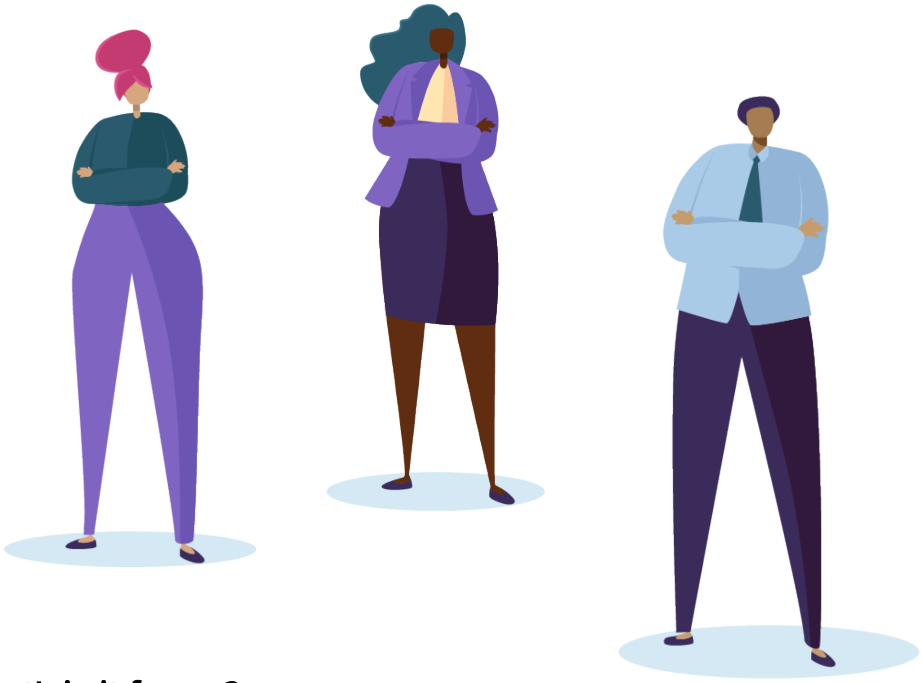
Cybersecurity Knowledge Assessment

The **Cybersecurity Knowledge Assessment** has been designed to help all employees of all skill levels across CMS get a better idea of how much they know about important cyber topics they're exposed to every day. Using the NIST Cybersecurity Framework as a template, the Cybersecurity Knowledge Assessment contains questions consisting of eleven different topics.

Features of the Cybersecurity Assessment include:

- An easy to use web interface (Typeform)
- Questions are based on phishing, threat actors and vectors, disaster recovery, PII/PHI, and more.
- The results of the Assessment will give the user an overall score and a score for each of the eleven different topics.
- Complete anonymity. Only the Assessment taker will see their score.
- Retakes. If you're unsatisfied with your score, you can return to it at any time to see how much you have improved.

You can find and take the Cybersecurity Knowledge Assessment at **https://cmsgov.typeform.com/to/H7UDuq9s**



What's in it for me?

For those who are less technically savvy, this Assessment will be a learning experience. As stated above, this Assessment has eleven different cybersecurity topics to learn about and give you a better idea what the cybersecurity world is really like. For those more experienced, this Assessment will be a nice refresher of concepts you may not have to use on a day-to-day basis.

ISSO Score Card

The **ISSO Score Card** is to give an ISSO the tools and information needed to maximize the many training opportunities that CMS offers. The Score Card instrument is a series of guided questions using the TypeForm application. At the end of the Score Card, each person taking the Score Card is presented with an overall score for the attempt, as well as scores for each of the subject areas within the Score Card.

More importantly, each ISSO is presented with a tailored set of training recommendations based on their answers to questions. Initially these training recommendations will be general, probably based on subject areas. In time, answers to each question will generate a training suggestion at the course/activity level.

Features of the Score Card include:

- Initially, approximately 30 questions, taking between 10 and 15 minutes. Questions will evolve as a better understanding of what questions to ask evolves. Note: questions are based directly on ISSO duties and responsibilities articulated in the IS2P and the IS2P2.
- Score Card results that give the user an overall score, and scores for each of the areas within the Score Card. (MVP)
- A custom-generated report that each user can take with them that presents results, along with suggested training (Initially on results screen (MVP); eventually a dedicated report). In follow on efforts training will have NICE crosswalks to allow users to find training themselves.
- Complete anonymity. Only the person taking the Score Card will see their results. (MVP)
- Multiple retakes. Over time, ISSOs' capabilities will improve, and training opportunities will become more specific. ISSOs can use the Score Card at any time to see how their capabilities have evolved, and what current training opportunities will most help them. (MVP and beyond)

You can find, and take, the ISSO Score Card at:
https://cmsgov.typeform.com/to/c67nf2Wr?typeform-source=cmsgov-ispg.typeform.com

Additional Training Opportunities

CMS ISPG Beneficiary Data Protective Initiative (BDPI)
The Beneficiary Data Protection Initiative's 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.

Federal Virtual Training Environment (Fed VTE)
Provides a free online, on-demand cybersecurity training system. Individuals with a .gov or .mil email address can register to use the system.

Health and Human Services Learning Management System (HHSLMS)
Provides over 3,000 Skill Soft courses, including cybersecurity certification preparatory training and continuing education unit (CEUs) and Books 24/7.

Information Assurance Support Environment (IA SE)
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
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.

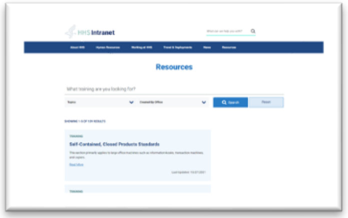
SPLUNK
Provides training on Splunk technology used to search, analyze, and visualize the machine-generated data gathered.

FORTINET
Fortinet is offering online training free of cost. Courses cover everything from basic cybersecurity awareness training to advanced training.

Links to Resources

Click

CMS ISPG Beneficiary Data Protection Initiative



Health and Human Services Learning Management System

Federal Virtual Training Environment

SANS
Cyber Security Training, Certifications, Degrees and Resources
Trusted Quality and Community

SANS

Information Assurance Support Environment

FORTINET

SPLUNK

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
Legal Advice and Advocacy (LGA)	Cyber Legal Advisor Privacy Officer/Privacy Compliance Manager	Provides legal advice and recommendations on relevant topics related to cyber law. 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.	731 732
Training, Education, and Awareness (TEA)	Cyber Instructional Curriculum Developer Cyber Instructor	Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs. Develops and conducts training or education of personnel within cyber domain.	711 712
Cybersecurity Management (MGT)	Information Systems Security Manager Communications Security (COMSEC) Manager	Responsible for the cybersecurity of a program, organization, system, or enclave. Individual who manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009) or key custodian for a Crypto Key Management System (CKMS).	722 723

NICE Category: Oversee and Govern (OV) - Continued

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 Manager 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
Digital Forensics (FOR)	Cyber Defense Forensics Analyst	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.	212