



**THIS
MONTH'S
FOCUS**

NATIONAL CYBERSECURITY AWARENESS MONTH

DID YOU KNOW?

Informed system users are the best line of defense against phishing, a serious high-tech scam that uses email to deceive recipients into disclosing sensitive information.

 CDSE – Center for Development of Security Excellence

 @TheCDSE

 Center for Development of Security Excellence

 Center for Development of Security Excellence

CDSE Pulse

Published by the Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) Outreach and Engagement Office.

DCSA Leadership

Daniel J. Lecce
Acting Director, DCSA

Kevin Jones Erika Ragonese
Assistant Director, Security Training *Deputy Assistant Director, Security Training*

CDSE Leadership

Heather Mardaga Glenn Stegall
Director *Deputy Director*

Pulse Staff

Samantha Dambach
Natalie Perkins
Content Developers/Managers

Isaiah Burwell Marc Pulliam
Content Writer *Content Designer*

NATIONAL CYBERSECURITY AWARENESS MONTH: 20 YEARS AND BEYOND

Cybersecurity is critical in our modern, digitally dependent culture. Even the most secure cyber spaces are at risk of an attack if the proper precautions are not taken. That is why in 2004, the President of the United States and Congress declared the month of October to be National Cybersecurity Awareness Month (NCSAM). This year marks the 20th anniversary of NCSAM, which is dedicated to the public and private sectors working together to raise awareness about the importance of cybersecurity.

This year's theme, "Secure Our World," calls on all Americans to adopt ongoing cybersecurity habits and improve online safety behaviors. Not only will "Secure Our World" remain a consistent theme for every Cybersecurity Awareness Month in the future, it will also launch as the Cybersecurity & Infrastructure Security Agency's (CISA) new cybersecurity awareness program. Its key messages underscore how we can secure our information, families, and businesses by focusing on four simple, yet critical, actions that

everyone should implement and continuously strengthen. There are several ways to secure our networks, but we will only mention a few here.

The first step is to use strong passwords and a password manager. Strong passwords are critical to protecting data. They should be long, random, unique, and include all four-character types (uppercase, lowercase, numbers, and symbols). Password managers are applications used for managing credentials. They can generate, store and share long, random, and unique passwords for each of your accounts in an encrypted database thereby increasing efficiency and improving security.

The second step is to enable multifactor authentication (MFA). Strong passwords alone may not be enough to protect your accounts, and enabling MFA provides an additional layer of security. An example of MFA is a

"Our increasingly interconnected, global cyberspace presents profound challenges in which we face 24/7/365 asymmetric, cyber threats with large scale real-world effects."

– CISA Strategic Plan 2023-2025





code sent to your phone or email that you must enter in addition to your password as part of the log in process for a website. This provides an extra layer of security that validates your identity. This is especially useful for email, social media, and financial accounts.

The third step is to recognize & report phishing. Phishing emails, texts, and calls are the number one way data gets compromised. Be cautious of unsolicited emails, texts, or calls asking for personal information. Avoid sharing sensitive information or credentials over the phone or email unless necessary, and don't click

on links or open attachments sent from unknown sources. Verify the authenticity of requests by contacting the individual or organization through a trusted channel. Report phishing attempts to the appropriate authorities or IT department. Learn to recognize the signs of phishing and report these incidents to protect data and devices.

The fourth step is to keep software updated. Ensuring your software is up to date is the best way to make sure you have the latest security patches and updates on your devices. Enable automatic updates and regularly check for updates manually if

automatic updates are not available. The four steps are a great foundation, but there are other tools to help build up cybersecurity for yourself and your organization.

CISA and the National Cybersecurity Alliance (NCA) have partnered to create resources and messaging for organizations to use when they talk with their employees, customers, and memberships about staying safe online. CISA also offers training opportunities for federal employees, partners, and citizens. Some of these training opportunities restrict availability or require registration, while others are open to the public.

CISA AND NCA CYBERSECURITY TRAINING AND RESOURCES

PRODUCT	DESCRIPTION
CISA NCSAM Website	Homepage for CISA NCSAM resources.
NCA NCSAM Website	Homepage for NCA NCSAM resources.
Cybersecurity Awareness Month 2023 Partner Toolkit	Resources and messaging for organizations to use when they talk with their employees, customers, and memberships about staying safe online.
Secure Our World Tip Sheets	Resources and advice to stay safe online in various languages.
Secure Yourself & Your Family	Information about staying safe online.
Secure Your Business	Information to protect businesses, employees, and customers with easy and effective security habits and policies.
Federal Virtual Training Environment	Free cybersecurity courses for the public, no login required.
Cybersecurity Training	Cybersecurity workforce training and education for federal employees, private-sector cybersecurity professionals, critical infrastructure operators, educational partners, and the general public.



The Defense Information Systems Agency (DISA) and the Center for Development of Security Excellence (CDSE) both offer cybersecurity training and security awareness resources for DOD and cleared industry.

DOD CYBERSECURITY TRAINING AND RESOURCES	
PRODUCT	DESCRIPTION
DOD Cyber Exchange Public	DISA's one-stop access to cyber information, policy, guidance, training, job aids, and cyber resources for cyber professionals throughout the DOD and general public.
Cybersecurity Catalog Webpage	CDSE's cybersecurity training and resources.
Cybersecurity Toolkit	CDSE's resources to help with cybersecurity responsibilities.

Cybersecurity is everyone's responsibility, and not just during NCSAM. Poor cyber practices can lead to financial loss or the loss of critical information. Individuals can strengthen their cybersecurity habits by consistently adopting the four critical steps for online safety outlined earlier. Organizations can provide cybersecurity training and awareness campaigns all year long to help their personnel learn and practice strong cybersecurity practices. Do your part to keep our Nation's cyberspace safe and secure!

NEW AND UPDATED CDSE CYBERSECURITY PRODUCTS

Risk Management Framework (RMF) CS100.CU. This curriculum, which introduces the RMF and explores how it is used to manage the overall risk to an organization from different sources, was updated with the release of seven new courses:

- Risk Management Framework (RMF) Prepare Step **CS101.16**
- Risk Management Framework (RMF) Categorize Step **CS102.16**
- Risk Management Framework (RMF) Select Step **CS103.16**
- Risk Management Framework (RMF) Implement Step **CS104.16**
- Risk Management Framework (RMF) Assess Step **CS105.16**
- Risk Management Framework (RMF) Authorize Step **CS106.16**

- Risk Management Framework (RMF) Monitor Step **CS107.16**

Students examine the framework components individually, enabling them to understand the entire process as it relates to their information system's entire lifecycle. This program focuses on providing practical guidance on completing and maintaining the certification and accreditation process and on obtaining formal authority to operate.





CYBERSECURITY EDUCATION COURSES

CDSE has established an education program of advanced and graduate courses designed specifically to broaden DOD security specialists' knowledge and understanding of the security profession and prepare them for leadership positions and responsibilities. All of the Education courses are tuition-free, offered in a virtual instructor-led environment, and open to U.S. military members and civilian government employees. Each completed course earns 160 Professional Development Units (PDUs) for use towards the maintenance of a Security Professional Education Development (SPeD) Program Certification. The courses also have the American Council on Education (ACE) CREDIT recommendations that may earn transfer credits at participating universities.

CDSE offers two Cybersecurity education courses:

The Future of Security Systems and Cybersecurity (ED510.10). This course is designed for the senior security managers. It addresses leading-edge technologies and their implications (positive and negative) for the field of security within DOD. It is designed to help security personnel thrive in an information systems environment.



Cybersecurity and Oversight of Information System Security (ED514.10). This course will explore the role of the non-technical DOD security specialist related to information systems security, information assurance and cybersecurity. Emphasis will be placed on developing effective relationships between the many organizational players who have a role in information systems security, information assurance, and cybersecurity and how these relationships serve to increase operational effectiveness and security of the organization.

Watch our **Education Program public service announcement** and visit our **website** to learn more about the program.

RECORDINGS AVAILABLE FOR DCSA CONFERENCES FOR DOD AND INSIDER THREAT

The 2023 Virtual DCSA Security Conference for DOD was held on August 16-17. This year's conference theme was "Elevating Security Through Vigilance and Innovation." The agenda topics included Insider Threat, controlled unclassified information, security classification guides, personnel security vetting, policy updates, and more. The conference was open to .mil and .gov email holders.

The Defense Counterintelligence and Security Agency Conference for Insider Threat in support of National Insider Threat Awareness Month (NITAM) was held on September 7. This event provided insider threat practitioners in DOD, federal agencies, private industry, critical infrastructure sectors, and academia with a virtual conference to engage with senior leadership on the topic of insider threat. This year's NITAM theme was "Bystander Engagement." The agenda included such topics as counter-insider threat professionalization, organizational resources, toolkits for insider threat mitigation, and more.

If you missed these events or would like to revisit the presentations, access the recordings in the **Conference Archive**.



NEW INDUSTRIAL SECURITY WEBCAST AVAILABLE

CDSE recently released a new recorded webcast “Tips for Submitting a Change Condition Package (CCP).” This 18-minute webcast provides guidance on acceptable National Industrial Security System (NISS) change condition package submissions for entities in the National Industrial Security Program. It also discusses the submission requirements for the following key areas: Changes in Ownership, Legal Structure, Name including DBA & AKA, Address, Key Management Personnel Essential, and Foreign Ownership, Control, or Influence (FOCI). Access the webcast [here](#).

UPCOMING WEBINARS

Sign up for the following upcoming live webinars:

An Alternative View of Preventing Insider Threats: Taking Culture Seriously

Thursday, November 2, 2023
12:00 to 1:30 p.m. ET

DC3 Mission Brief and Current Cyber Threats

Thursday, November 16, 2023
1:00 to 2:30 p.m. ET

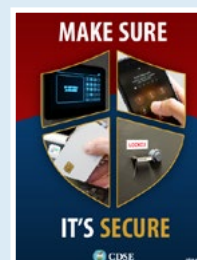
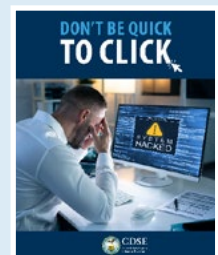
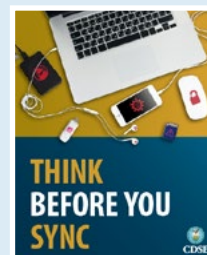
The Enemy Within: A Case Briefing

Wednesday, December 13, 2023
12:00 to 1:30 p.m. ET

Visit CDSE’s [webinar webpage](#) to register for these events and join the discussion!

NEW INDUSTRIAL SECURITY POSTERS NOW AVAILABLE





Check out CDSE’s recently released new **security awareness posters**:

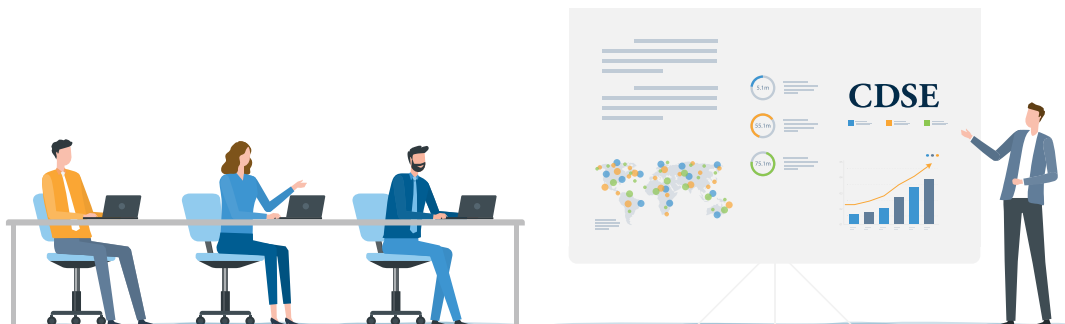




FY 2024 UPCOMING COURSES

CDSE released the FY 2024 course schedule in August. Consider signing up for one of CDSE’s instructor-led training (ILT) or virtual instructor-led training (VILT) courses! Training is free and the VILT eliminates travel expenses. Complete CDSE courses to earn professional development units (PDUs) toward maintenance of Security Professional Education Development (SPeD) Program certifications and credentials. Select courses have the American Council on Education (ACE) CREDIT recommendations that may earn transfer credits at participating universities. Classes fill quickly, so get an early start in planning your security training for FY24. Access the [training schedule](#) today to learn more! Below is a list of ILT/VILT courses available from February 2024 to April 2024.

COURSE	DATE	DESCRIPTION
Physical Security and Asset Protection	Mar. 25 - Apr. 14, 2024 (VILT) Apr. 29 - May 3, 2024 (ILT)	This course will provide students the ability to identify and utilize regulatory guidance, methodologies, and concepts for protecting DOD assets.
Getting Started Seminar for New Facility Security Officers	Apr. 16 - 19, 2024 (VILT)	This course allows new Facility Security Officers (FSOs) and security personnel to learn and apply fundamental National Industrial Security Program (NISP) requirements in a collaborative environment. It also serves as a refresher on industrial security basics for experienced FSOs.
DOD Security Specialist 	Feb. 6 - 14, 2024 (ILT) Mar. 5 - 13, 2024 (ILT)	This course provides students a baseline knowledge to perform common DOD security tasks and practices.
Introduction to Special Access Programs 	Mar. 5 - 8, 2024 (ILT) Mar. 12 - 15, 2024 (ILT) Apr. 1 - 9, 2024 (VILT)	This course focuses on the DOD Special Access Program (SAP) fundamentals and is designed to prepare students to become SAP security professionals.
Assessing Risk and Applying Security Controls to NISP Systems 	Mar. 18 - 22, 2024 (ILT)	This course provides students with guidance on applying policies and standards used throughout the U.S. Government to protect information within computer systems, as delineated by the Risk Management Framework (RMF) process. This course will also provide a comprehensive understanding of contractor requirements under the National Industrial Security Program (NISP).
Orientation to SAP Security Compliance Inspections 	Feb. 21 - 22, 2024 (ILT)	This course provides students with policy and direction to ensure inspections are standardized, equitable, and consistent across inspection agencies utilizing the DOD Special Access Program (SAP) Security Manuals.





WHAT THE STUDENTS ARE SAYING

THE FUTURE OF SECURITY SYSTEMS AND CYBERSECURITY (ED510.10):

"I am able to better communicate with our cyber personnel."

"Opportunities for collaborative learning through projects, group assignments, and discussions that enable students to share their viewpoints, knowledge, and skills with others and receive feedback, participate in constructive debates, and learn about different perspectives."

"This class helped me to understand in greater detail how to balance potential threats with the mitigation process."

"Discussion forum topics were interesting. I liked Dr. Hestermann weaving together fundamentals with new, emerging trends in cyber."

CYBERSECURITY AND OVERSIGHT OF INFORMATION SYSTEM SECURITY (ED514 .10):

"This course exceeded my expectations. The knowledge of the instructor and the wealth of resources and instructions provided was greater than I expected."

"I learned how to draft a security plan which I had never done before."

"I gained more insight on cyber requirements."



CDSE NEWS

CDSE offers an email subscriber news service to get the latest CDSE news, updates, and information. You may be receiving the Pulse through your subscription, but if you were forwarded this newsletter from another source and would like to subscribe to the Pulse or one of our other topics, visit our [news page](#) and sign up or update your account today.

Insider Threat Bulletins	Weekly Flash	Quarterly Product Update
---------------------------------	---------------------	---------------------------------

