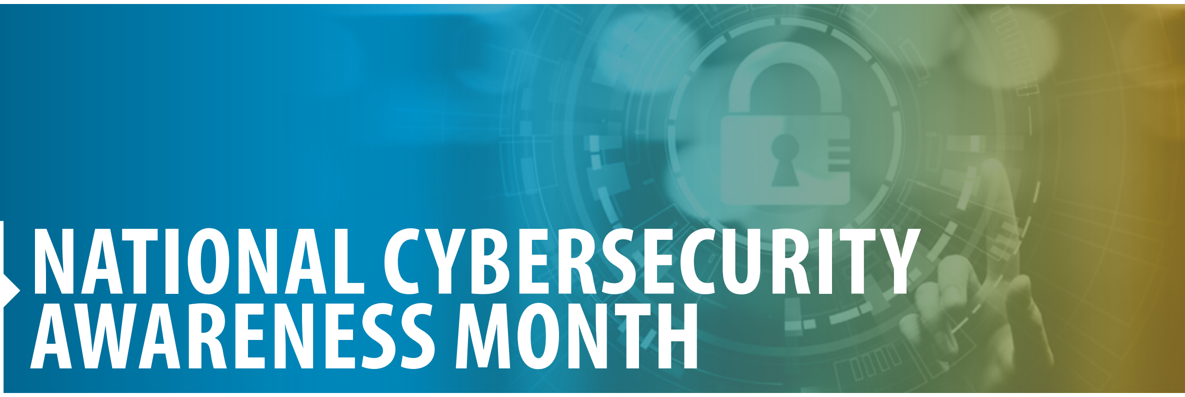
CDSE pulse
VOLUME 3 ISSUE 10
October 2022



THIS MONTH'S FOCUS

NATIONAL CYBERSECURITY AWARENESS MONTH

DID YOU KNOW?

The Internet Crime Complaint Center reported a 7% increase in cyber complaints in 2021 with potential losses exceeding $6.9 billion.

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

CDSE Pulse

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

DCSA Leadership

William K. Lietzau
Director, DCSA

Daniel Lecce
Deputy Director, DCSA

Kevin Jones
Assistant Director, Training

Erika Ragonese
Deputy Assistant Director, Training

CDSE Leadership

Heather Mardaga
Director

Pulse Staff

Adriene Brown
Chief Content Officer

Samantha Dambach
Natalie Perkins
Content Developers/ Managers

Isaiah Burwell
Content Writer

Marc Pulliam
Content Designer

SEEING YOURSELF IN CYBER

The National Cybersecurity Awareness Month (NCSAM) has seen immense growth since its inception 19 years ago. The initiative which started under leadership from the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA) now reaches federal/state/local government agencies, U.S. armed services, consumers, small and medium-sized businesses, corporations, educational institutions, and people across the Nation. This article will look back at the history of NCSAM, why it is important, and how you can contribute as the month continues to build momentum.

NCSAM launched in October 2004 as a broad effort to help all Americans stay safe and secure online. In subsequent years, leading administration officials from the DHS, the White House, and other agencies have regularly participated in events across the United States. In 2010, the kickoff of NCSAM also included the launch of the STOP. THINK. CONNECT. campaign. NCSAM operates similarly to a grassroots campaign with participation from a multitude of government, industry, and academic partners that encourage their employees, stakeholders, customers, students, and the public to increase their cybersecurity awareness and knowledge of best practices.

This year's campaign theme is "*See Yourself in Cyber*" and demonstrates while cybersecurity may seem like a complex, technical subject, it is really about people. *See Yourself in Cyber* means you take cybersecurity seriously no matter what role you play. Employees have a responsibility to protect their organization's online information by following cybersecurity policies, guidance, and best practices. Individuals can take basic steps to protect their online information and privacy. Government and cleared industry security professionals can take ownership of their role protecting information, brand, and reputation, by adhering to required cybersecurity policies and guidance in the workplace. Additionally, security managers and facility security officers can promote cybersecurity training with their workforces. Establishing security awareness programs is another way

> "To build a more resilient Nation, everyone—from K through Gray—has a role to play, which is why our theme for this year's Cybersecurity Awareness Month is 'See Yourself in Cyber,'" said CISA Director Jen Easterly. "This October, we are taking this message directly to the American people because whether you're a network defender or anyone with an internet connection, we all have a role to play in strengthening the cybersecurity of our Nation."

Additional Activities to Support NCSAM

- Email campaign to colleagues, employees, customers and/or students
- Host a poster/video contest for employees/students in which participants create informative online safety resources
- Work with your leadership to issue an official proclamation to show your organization's support of the month
- Host a local or virtual event, or training for your organization or community to discuss smart computer practices and relevant cybersecurity issues (best security practices for email, social media, and/or online transactions)
- Join the cause by becoming an individual or organization sponsor on the National Cybersecurity Alliance website or a CISA partner on the CISA Cybersecurity Awareness website
- Sign up for the CISA Community Bulletin - **https://www.cisa.gov/join-cisa-cybersecurity-awareness**

organizations enhance strong cybersecurity practices among their workers. These steps help prevent cyber incidents at work or further down the supply chain. Critical infrastructure owners and operators are part of a larger network of functions and systems that play a part in ensuring cybersecurity for the larger ecosystem.

No matter the age or occupation, everyone can make a difference during NCSAM. There are several training and security awareness resources that explain the importance of these steps and how to implement them available on the DOD Cyber Exchange (public version), the Cybersecurity and Infrastructure Security Agency (CISA), the National Cybersecurity Alliance, and the CDSE websites. Resources include articles, posters, and job aids and can be accessed by individuals and organizations. The websites also contain a wealth of additional cybersecurity training and awareness resources on other topics that can be viewed and shared during October and throughout the year.

Individuals and organizations can also follow CDSE, CISA, and the National Cybersecurity Alliance on Twitter, Facebook, YouTube, and LinkedIn and subscribe to email updates to receive and share the latest online cybersecurity news and resources. Also, you can post your own online safety tips and reminders about NCSAM on your social networks. Individuals and organizations with blogs or podcasts can share cybersecurity information in October by highlighting one of the NCSAM's calls to action.

Even though the majority of Americans have access to the internet, it does not mean everyone is knowledgeable about cybersecurity. By sharing NCSAM's information and messaging, we can expose more people to the best online safety practices. The future of cybersecurity should not be about one organization protecting everyone from cyber threats; it should be about people protecting themselves and their organizations.

Four key action steps you can take to improve your cybersecurity posture include:

- enabling multi-factor authentication
- using strong passwords
- recognizing and reporting phishing
- updating your software

DOD RESOURCES

PRODUCT	URL
Cyber Training	**https://public.cyber.mil/cyber-training/**
Do's and Don'ts of Network Utilization and Cybersecurity: Defend the DODIN	**https://dl.dod.cyber.mil/wp-content/uploads/covid19/pdf/unclass-cyber_and_networking_dos_and_donts.pdf**
Top Telework Tools	**https://dl.dod.cyber.mil/wp-content/uploads/covid19/pdf/unclass-top_telework_tools-PUBLIC.pdf**
Phishing Warfare Brochure	**https://dl.dod.cyber.mil/wp-content/uploads/trn/products/brochures/unclass-phishing_brochure.pdf**
Mobile Device Usage Poster	**https://dl.dod.cyber.mil/wp-content/uploads/trn/products/posters/Poster-Mobile_Device_Do_This_Not_That.pdf**
Cybersecurity Training Catalog	**https://www.cdse.edu/Training/Cybersecurity/**
Cybersecurity Toolkit (Training and Awareness Tab)	**https://www.cdse.edu/Training/Toolkits/Cybersecurity-Toolkit/**
Cybersecurity Posters	**https://www.cdse.edu/Training/Security-Posters/Cybersecurity/**

CISA RESOURCES

PRODUCT	URL
CISA Cybersecurity Awareness Month Website	**https://www.cisa.gov/cybersecurity-awareness-month**
Cybersecurity Awareness Month 2022 Public Toolkit	**https://www.cisa.gov/sites/default/files/publications/CAM22_PublicToolkit_FINAL_OCC_CSD_DIR_508c.pdf**
CISA Multi-Factor Authentication	**https://www.cisa.gov/mfa**
Choosing and Protecting Passwords	**https://www.cisa.gov/uscert/ncas/tips/ST04-002**

NATIONAL CYBERSECURITY ALLIANCE RESOURCES

PRODUCT	URL
National Cybersecurity Alliance Cybersecurity Awareness Month Website	**https://staysafeonline.org/programs/cybersecurity-awareness-month/**
About Cybersecurity Awareness Month (History)	**https://staysafeonline.org/programs/about-cybersecurity-awareness-month/**
Multi-Factor Authentication	**https://staysafeonline.org/online-safety-privacy-basics/multi-factor-authentication/**
Passwords	**https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/**
Resources and Guides	**https://staysafeonline.org/resources/**

FBI RESOURCES

PRODUCT	URL
FBI Cyber Crime	**https://www.fbi.gov/investigate/cyber**
FBI Internet Crime Complaint Center IC3	**https://www.ic3.gov/**
FBI/IC3 2021 Internet Crime Report	**https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf**

CDSE FY23 TRAINING COURSE SCHEDULE

As you are planning your annual training, consider signing up for one of CDSE's instructor-led (ILT) or virtual instructor-led (VILT) courses. Training is free and the VILT option eliminates travel expenses. CDSE courses earn Professional Development Units (PDUs) toward maintenance of Security Professional Education Development (SPēD) Program certifications and credentials. Select courses with American Council on Education (ACE) credit recommendations may earn transfer credits at participating universities. Additionally, the DOD Security Specialist course is approved for Continuing Education Unit (CEU) credit toward several CompTIA certification renewals. Access the **training schedule** to learn more!

REGISTER FOR SPRING EDUCATION CLASSES

Registration will open October 31st for the spring semester of CDSE Education classes that run from January 23 to May 21, 2023. Classes fill quickly, so please register early to secure your spot in the spring semester.

CDSE Education Program offers:

- Tuition-free, flexible and 100% virtual instructor-led courses
- Real-world practical assignments
- Virtual networking with professionals throughout the security community
- Five Security Education Certificate programs
- Highly qualified instructors

You can learn more about the available classes and register for them by accessing the links here: **https://www.cdse.edu/education/courses.html**

To register, log into STEPP via: **https://cdse.usalearning. gov/login/index.php**

If you have any questions, or need additional information, contact the CDSE Education Program at: **dss.ncr.dss-cdse.mbx.cdse¬education@mail.mil**

CERTIFICATION PROGRAM UPDATES

CDSE has released several SPēD Certification program updates and products in the last six months:

The new certification maintenance and renewal policies/procedures (**https://www.cdse.edu/Portals/124/Documents/certification/sped-program-certification-maintenance-guidelines.pdf**) went into effect on October 1st. These new policy changes include:

- Professional Development Units (PDUs) based on level of effort
- Updated and expanded PDU categories
- Single expiration date across all certifications/ credentials
- Single CRF form
- Maintenance periods based upon the candidate initiating an action (e.g., submitting a form in the My SPēD system or attaining a new SPēD Certification). This period remains at two years for each cycle

The Certification Renewal Form (CRF) has been updated to align to the new maintenance guidelines

The SPēD and APC candidate handbooks have been merged, reformatted, and refreshed: **https://www.cdse.edu/Portals/124/Documents/certification/DOD-Professional-Certification-and-Credentialing-Handbook.pdf**

The new Antiterrorism Credential (ATC) is now available **https://www.cdse.edu/Certification/About-SP%C4%93D-Certification/Antiterrorism-Credential/**

DECEMBER CYBERSECURITY INSTRUCTOR-LED COURSE

The next "Assessing Risk and Applying Security Controls to NISP Systems," instructor-led course is scheduled to start December 5, 2022. This five-day course provides students with guidance on applying policies/standards used to protect information within computer systems, as delineated by the Risk Management Framework (RMF) process. Learn more at **https://www.cdse.edu/Training/Instructor-led/CS301/**

★★★★★ WHAT THE SECURITY COMMUNITY IS SAYING

Introduction to the Risk Management Framework (RMF) (CS124.16) (eLearning)

"I really appreciated the governance and tier1-3 breakdown regarding role assignment and AO clarification. Also I like the pertinent legislations and their listed authorities being included as well. This is one of the best if not the best intro to RMF training I've taken."

Cybersecurity Awareness (CS130.16) (eLearning)

"Keep the updated (new) scenarios coming. It is refreshing to see and test my knowledge on emerging threats. . ."

"I think this was a very useful course and contains real life situations in which we need to keep an eye out for. Definitely learned a lot from this and will retain the information as I continue working."

2022 VIRTUAL DOD SECURITY CONFERENCE

The 2022 Virtual DOD Security Conference was held October 12-13 and drew nearly 2,000 participants. This year's conference theme was "Developing a Resilient Security Workforce in a Changing Environment" and 30% of attendees were participating for the first time. The agenda included policy change and implementation updates on topics such as security in a digital world, operations security, controlled unclassified information, personnel security policy, PERSEREC studies, and more. If you missed the conference or would like to revisit the presentations, the recordings will be posted later in the CDSE Conference Archive. An announcement will be released in the Pulse and the Flash when recordings are available. Please note, you must have a .mil or .gov email for access to recordings.

Disclaimer: The editorial content of this publication is the responsibility of the Center for Development of Security Excellence Marketing and Communications Office.