CDSE
LEARN. PERFORM. PROTECT.

PULSE

VOLUME 6 ISSUE 10 | October 2025

CDSE Pulse
Published by the Security Training Directorate Outreach and Engagement Office for the Center for Development of Security Excellence (CDSE).

DCSA Leadership
Daniel J. Lecce
Deputy Director, DCSA

Kevin Jones
Assistant Director, Security Training

Erika Ragonese
Deputy Assistant Director, Security Training

CDSE Leadership
Audrey Gutierrez
Director

Glenn Stegall
Deputy Director

Pulse Staff
Cashmere He
Chief Content Officer

Matt Wright
Content Writer

Jenise Kaliszewski
Tammi Bush
Content Contributors

Marc Pulliam
Content Designer

Center for Development of Security Excellence

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

THIS MONTH'S FOCUS

Cybersecurity: Awareness as the First Line of Defense

By Matt Wright

LINTHICUM, Md. - The digital landscape is rapidly changing, and so are the tactics used by America's adversaries.

A large portion of today's battles take place in the cyber realm rather than by land or sea. Adversaries continually launch dangerous attacks on everything from power grids and networks to states themselves.

In August, Nevada state websites and services were disabled after a ransomware attack, shutting down the Department of Motor Vehicles both in-person and online.

During the same timeframe, the National Security Agency (NSA) released a **press release** regarding China state-sponsored actors targeting critical infrastructure such as telecommunications, transportation, lodging, and military networks globally.

Due to these attacks and others carried out every day, it's important to be aware of ways to mitigate and decrease risks.

Since 2004, October has been dedicated as Cybersecurity Awareness Month, a collaborative campaign for public and private sectors to raise awareness about the importance of cybersecurity.

Launched by the National Cybersecuity Alliance and the U.S. Department of Homeland Security, Cybersecurity Awareness Month encourages actions to reduce online risk and generate discussions on global cyber threats.

The Cybersecurity & Infrastructure Security Agency (CISA) advises online users to act in four ways.

The first recommendation is to use strong passwords. Strong passwords are long, random, and unique and include all four-character types (uppercase, lowercase, numbers, and symbols).

The second is multi-factor authentication. This step goes beyond creating a strong password by confirming the user's identity when logging in to our accounts. Examples include entering a code texted to a phone or one generated by an authenticator app.

The third is recognizing and reporting phishing attempts. Be cautious of unsolicited messages asking for personal information. Avoid sharing sensitive information or credentials with unknown sources. Report phishing attempts and delete the message.

The fourth and final tip is updating software. Regular updates ensure users have the latest security patches and updates on their device.

For more in-depth training, CDSE offers a multitude of cybersecurity awareness resources and training options.

The **Assessing Risk and Applying Security Controls to NISP Systems** instructor-led course provides students with guidance on applying policies and standards to protect information within computer systems. The course also provides a comprehensive overview of contractor requirements under the National Industrial Security Program (NISP). The five-day course is offered several times through the year at CDSE in Linthicum, Md.

CDSE also offers a **Cybersecurity Toolkit** containing resources related to policy, system management, incident response, social media, and much more. It has job aids, posters, games, and videos to assist in forming or tailoring a cyber awareness campaign.

When it comes to self-paced eLearning courses, choose from **Introduction to the NISP RMF A&A Process** (CS150.16), **Phishing and Social Engineering: Virtual Communication Awareness Training** (DS-IA103.06), **Cybersecurity for Security Personnel** (CS160.16), amongst other educational offerings. A full list of cybersecurity resources offered at CDSE can be found **here**. Check with COMPTIA to find out about Continuing Education Units eligibility.

As the first line of defense, cybersecurity awareness requires vigilance beyond the month of October. It is a 24-hour, 365 day-a-year effort. As America's adversaries continue to evolve and adapt, CDSE will be there every step of the way, providing resources and training to help mitigate threats.

CYBERSECURITY

New Short: Cybersecurity Defense in Depth

A new "**Cybersecurity Defense-in-Depth**" short was released in late September to introduce the Defense-in-Depth in cybersecurity concept and demonstrate how multiple layers of security controls work together to protect networks and critical systems from cyber threats.

The target audience for this short is the Defense Security Enterprise, including facility security officers (FSO), information systems security professionals (ISSP), and cybersecurity system engineers.

Updated Course: Introduction to the Risk Management Framework (RMF) CS124.16

A new e-learning course titled "**Introduction to the RMF**," is now available. This course identifies policies and regulations governing the RMF process and details the seven-step implementation process and how it applies to the acquisition process. The course is available on STEPP as well as the **Security Awareness Hub** and includes a test-out option.

The course is intended for military, civilian, and contractor personnel responsible for evaluating information systems under the RMF and certifying that information systems meet security requirements.

Instructor-Led Training: Assessing Risk and Applying Security Controls to National Industrial Security Program (NISP) Systems (CS301.01)

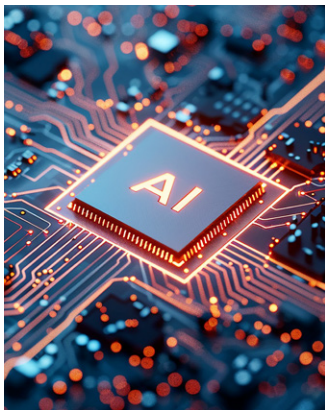
The cybersecurity team is offering a new training, "**Assessing Risk and Applying Security Controls to NISP Systems**." This course provides guidance on applying policies to protect information delineated by the RMF process and a comprehensive review of contractor requirements under the NISP.

The target audience for this training includes information system security managers (ISSMs), information system security officers (ISSOs), and facility security officers (FSOs) involved in the planning, management, and execution of security programs for cleared industry.

In-person courses will be offered Linthicum, Md. on the following dates:

- Nov. 3-6, 2025
- Feb. 2-6, 2026
- May 4 - 8, 2026
- Aug. 17-21, 2026

The Impacts of Artificial Intelligence and Emerging Technologies on the Cybersecurity Landscape Webinar



Join the new webinar, "**The Impacts of Artificial Intelligence and Emerging Technologies on the Cybersecurity Landscape**," on Wednesday, Oct. 15 from 11:00 am - 12:00 pm ET. The unclassified webinar is open to military, federal government, and industry professionals.

The introductory webinar will focus on the impact of artificial intelligence and emerging technologies on the cybersecurity landscape. Primary features include new AI policies and guidelines as well as best practices for AI models.

INDUSTRIAL SECURITY

Industrial Security Posters

Three posters are now available on the CDSE website:

- Know Security, No Incidents
- Think Before You Sync
- Don't Be Quick to Click

The posters are available for download and to raise security awareness in the workplace.

INSIDER THREAT

CDSE Releases 100th Case Study

CDSE hit a major milestone by recently releasing the 100th case study profiling **Ji Chaoqun**. Chaoqun is a Chinese citizen who came to the U.S. from Beijing, China in August 2013 on an F1 visa. Chaoqun holds a master's degree in electrical engineering from the Illinois Institute of Technology in Chicago.

Ji enlisted in the U.S. Army Reserves under the Military Accession Vital to the National Interest (MAVNI) program in 2016. During his time in the reserves, high-level intelligence officers from the Jiangsu Province Ministry of State Security (JSSD) recruited Chaoqun as part of an effort to obtain access to advanced aerospace and satellite technologies being developed by U.S. companies. In 2023, Chaoqun was convicted of acting illegally within the United States as an agent of the People's Republic of China and was sentenced to eight years in prison.

With the release of the 100th case study, CDSE cements the position as the premier providers of security training to the federal government and industry partners. Audrey Gutierrez, CDSE director, remarked "reaching 100 case studies reflects not just hard work,

but creativity, persistence, and a real commitment to excellence. I'm grateful for the standard set by our team. I'm proud of the impact this work continues to have."

This achievement is not only a credit to the instructors, instructional system designers (ISDs) and curriculum managers, but also to the web team, editors, designers, and outreach and engagement. CDSE case studies have had over 120,000 views on the CDSE website.

Case studies profile individuals sentenced for counterintelligence, cyber or insider threat crimes and include a short summary of the crime, indicators, and outcome or conviction.

Two New Courses Coming Soon!

Supervisor and Command Leader Awareness of Insider Risk (INT215)

"Supervisor and Command Leader Awareness of Insider Threat Risk" is under development to be released soon. The course will provide realistic scenarios and examples of insider threat behavior and how organizational culture, proactive engagement, and leadership actions play a role in risk mitigation.

Establishing an Insider Threat Program for Your Organization (INT122.16)

A new "Establishing an Insider Threat Program for Your Organization" e-Learning course is planned for release in November. The course will provide practical guidance on developing compliant insider threat programs.

FY26 Insider Threat Detection Analysis Course (ITDAC) Schedule Released

CDSE released the FY26 schedule for the highly acclaimed "Insider Threat Detection Analysis Course" (ITDAC), specifically designed for insider threat analysts. The virtual course will be offered on the following dates:

- Oct. 20-24, 2025
- Jan. 12-16. 2026
- Feb. 16-20, 2026
- March 16-20, 2026
- April 13-17, 2026
- May 11-15, 2026
- June 15-19, 2026
- July 13-17, 2026
- Aug. 17-21, 2026
- Sept. 21-25, 2026

ITDAC provides counter-insider threat analysts hands-on practice applying critical thinking skills and structured analytic techniques to potential insider threat indicators. The course uses simulated insider threat cases to analyze reports, seek additional information, build context, and develop effective mitigation strategies. To register, click **here**.

PHYSICAL SECURITY

Physical Security and Asset Protection (PY201.10)

From Oct. 20 to Nov. 7, CDSE will host the "Physical Security and Asset Protection" five-day virtual course which equips students with the expertise to identify vulnerabilities, develop comprehensive security plans, and protect people, equipment, facilities, activities, and operations (PIE-FAO).

There are 11 prerequisite eLearning courses and exams that lay the foundation for the course, providing a comprehensive introduction to the Physical Security Program. All prerequisites must be completed prior to enrollment in the course.

Review prerequisites and register for the **Physical Security and Asset Protection** (PY201.10) course via STEPP.

SPECIAL ACCESS PROGRAMS

FY26 Special Access Programs Course Calendar Released

The FY26 Special Access Program (SAP) training calendar for "Introduction to SAPs" is now available. The course introduces new SAP security professionals to the security requirements outlined in the DoDM 5205.07 utilizing practical exercises. Both **in person** and **virtual** training options are available.

SAP Markings Short

The CDSE SAP team released an updated **SAP Markings short**. This short covers SAP specific markings as outlined in DoDM 5200.01 volume 2. This short will outline the appropriate markings, as well as how to recognize and apply control markings.

INFORMATION SECURITY

Activity Security Manager INFOSEC VILT Course Schedule for FY26

The "**Activity Security Manager INFOSEC**" VILT course (IF203.10) provides students with knowledge to implement information security policies and procedures to mitigate and manage risks associated with developing, managing, and evaluating an information security program (ISP). Lessons emphasize key activity security manager responsibilities in relation to protecting classified national security information and controlled unclassified information (CUI).

This mid-level course includes security classification, downgrading, declassification, safeguarding and handling, access and dissemination control, accountability, storage, disposal, destruction, transmission and transportation, security incidents, and security education and training awareness. Register **here** to secure your spot!

Information Security: Updated Products

CDSE published updated versions of the following products:

"**Transmission and Transportation for DOD**" (IF107.16) eLearning course offers a more interactive scenario based instructional course to effectively implement regulatory guidance.

NOFORN REL/TO job aid replaces the CDSE NOFORN/REL trifold with quick reference and scenario-based examples to support implementing regulatory guidance and dissemination control markings.

Original Classification Authority (OCA) desktop reference reflects new policy guidance for the original classification process communicated in the January 2025 issuance of DODM 5200.45, Original Classification

Authority and Writing a Security Classification Guide. It provides a quick reference and scenario-based examples regarding original classification process.

Marking Syntax for U.S. Classified Information job aid addresses correct marking syntax for classified information in accordance with regulatory guidance. The job aid supports the CDSE Marking Syntax short.

FY 2026 UPCOMING COURSES

Registration Now Open

CDSE courses are a great way to gain security knowledge, gain awareness, and expand skill sets. Secure your spot now as classes fill quickly!

Cybersecurity
Assessing Risk and Applying Security Controls to NISP Systems (CS301.01)
- November 3 - 6, 2025 (Linthicum, Md.)

Industrial Security
Getting Started Seminar for New Facility Security Officers (IS121.10)
- Oct. 21 - 24, 2025 (Virtual)

Insider Threat
Insider Threat Detection Analysis Course (INT200.10)
- Oct. 20 - 24, 2025 (Virtual)

Physical Security
Physical Security and Asset Protection (PY201.10)
- Oct. 20 - Nov. 7, 2025 (Virtual)

Special Access Programs
SAP Mid-Level Security Management Course (SA201.01)
- Nov. 3 - 7, 2025 (Linthicum, Md.)

UPCOMING WEBINARS

The Impacts of Artificial Intelligence and Emerging Technologies on the Cybersecurity Landscape

Wednesday, Oct. 15, 2025 | 11:00 am to 12:00 pm ET

Click **here** to register

STAFF SPOTLIGHT

Meet Ashley Benitez, Training Specialist, Cybersecurity

By Tammi Bush

As a cyber team training instructor, Ashley Benitez has made lasting contributions to the Center for Development of Security Excellence (CDSE) in just nine short months on the job. Her direct responsibilities include instructing and serving as the course manager in the instructor-led training course "Assessing Risk and Applying Security Controls to NISP Systems." She works closely with the cyber team to revise and create cyber training materials to support the mission of CDSE.

Benitez' role as a training instructor strengthens the department's security posture by delivering quality security training and education to professionals across the federal government and industry. Benitez aids in upholding protections of national security information, various assets, and performance of sensitive duties as set forth by the department's critical missions.

Benitez applied to work at CDSE to continue her career in public service and cybersecurity education. Previously, Benitez served as a secondary computer science and cybersecurity teacher. In 2023, Benitez was one of 15 esteemed STEM educators selected for the Albert Einstein Distinguished Educator Fellowship (AEF). She served as the AEF Fellow and subject matter expert within the Academic Engagement Branch at the Cybersecurity Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS). At CISA, Benitez was able to support K12 cybersecurity and cyber workforce development initiatives on a national scale. Seeing the impact of her work inspired her to continue her public service and national impact in cybersecurity education.

Through the expertise and contributions of staff like Benitez, CDSE can provide a broader impact on cybersecurity education across the enterprise. Benitez was part of a joint effort to develop the upcoming "**Impacts of Artificial Intelligence and Emerging Technologies on the Cybersecurity Landscape**" webinar scheduled for Oct. 15, from 11:00 am to 12:00 pm ET, which addresses influences of emerging technologies on the cybersecurity landscape.

Benitez and her team also created new job aids such as an updated Social Media Safety Smart Card, Plan of Action and Milestones (POA&M) job aid, Security Configuration Assessment of Information Systems job aid, and the new Identifying Phishing Smart Card. These job aids can be found on the **CDSE Cybersecurity Job Aids Page**.

Benitez plays a key role in educating security professionals on cybersecurity practices, a vital aspect of protecting national security. Her passion and commitment to the mission are evident in the unwavering dedication and expertise she brings to DCSA.

CDSE NEWS

Update: 2025 DCSA Security Conference for DOD

Session recordings from 2025 DCSA Security Conference for Department of Defense are now available. Registered participants can access the recordings by clicking **here**.

STEPP Transitions to D-ICAM Access on October 1, 2025

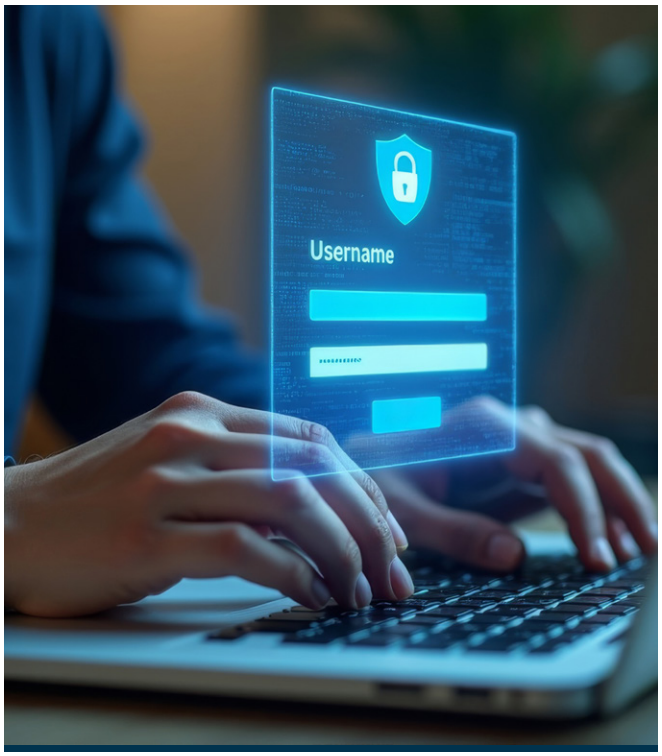
Effective 01 OCT, Security Training, Education, and Professionalization Portal (**STEPP**) will transition from direct login to DCSA Information Systems Agency Identity, Credential, and Access Management (**D-ICAM**) access.

This change affects all STEPP username and password users.

To Access STEPP on October 1, 2025:

1. Navigate to D-ICAM at **https://icam.dcsa.mil/**
2. Select "Accept"
3. At the bottom, select "Don't have an account? Sign up"
4. Enter First Name, Last Name, e-mail address associated with STEPP, and enter a password. Then choose "Sign Up".
5. You will receive an e-mail verification from noreply@okta.mil. Select "Verify your email" or "Enter a verification code instead". Either option will work. Follow the instructions.
6. Select "Continue" to proceed to the D-ICAM dashboard and choose the STEPP tile.

***NOTE**: There is an option to set up an authentication method. If you choose the authentication - "Okta Verify" - this involves scanning a barcode. Not all individuals will have the ability to do this, and it is optional at this time.*



Need Help?

- General Guidance: Select the "Help" link on the D-ICAM login screen.
- D-ICAM Authentication Issues: For problems creating or accessing a D-ICAM account, email: **dcsa.itsupport@mail.mil** or call 878-274-1344.
- STEPP Login Issues: Submit a **help desk ticket** and select "Access - Unable to access via username and password."

ABOUT DCSA

The Defense Counterintelligence and Security Agency (DCSA) provides industrial security engagement and counterintelligence support to secure the trustworthiness of the U.S. government's workforce, contract support, technologies, services, and supply chains.

Our Role
We protect America's trusted workforce, trusted workspaces, and classified information. To do so, we have two fundamental missions: personnel security and industrial security. Supporting these two core missions are counterintelligence and insider threat and security training. For over 50 years, our agency has used each of these missions to meet the threats of our nation's adversaries.

How We Serve
DCSA is the largest investigative service provider in the federal government, supporting over 100 federal entities. We oversee 12,500 cleared facilities under the National Industrial Security Program (NISP). We rely on the following directorates to ensure the security of our nation's technologies and information.

Personnel Security
We deliver efficient and effective background investigations, continuous vetting, and adjudications. In doing so, we safeguard the integrity and trustworthiness of the federal and contractor workforce. We conduct background investigations for 95% of the federal government, including 105 departments and agencies. We also adjudicate 70% of the federal government's adjudicative determinations.

Industrial Security
At DCSA, we oversee 12,500 cleared facilities under the National Industrial Security Program (NISP). We make sure companies are protecting their facilities, personnel, and associated IT systems from attacks and vulnerabilities.

Counterintelligence and Insider Threat
Counterintelligence and insider threat supports both our personnel security and industrial security missions. Counterintelligence focuses on foreign insider threat while insider threat is focused on internal threat. In this mission center, we identify and stop attempts by our nation's adversaries to steal sensitive national security information and technologies.

Security Training
Our agency is comprised of nationally accredited training centers. These centers provide security training, education, and certifications for security professionals across the federal government and industry.

CDSE CONTACT LIST

Mailing/Postal Address
938 Elkridge Landing Road
Linthicum, Md 21090

STEPP (Learning Management System) Help Desk
Submit an online support request ticket or call the Help Desk at 202-753-0845 within the Washington, DC area or toll free at 833-200-0035 on weekdays from 8:30 a.m. to 6:00 p.m. Eastern Time.

508 Compliance and Accessibility
cdseaccessibility@mail.mil

Certification Division/SPēD Project Management Office
dcsa.spedcert@mail.mil

Education Division
dcsa.cdseeducation@mail.mil

Outreach and Engagement Office
dcsa.ncr.cdse.mbx.cdse-communications@mail.mil

Training Division
dcsa.cdsetraining@mail.mil

Webinars
dcsa.cdsewebinars@mail.mil

Webmaster
dcsa.cdseweb@mail.mil

Still not sure whom to contact?
dcsa.ncr.dcsa-cdse.mbx.cdse-front-office@mail.mil