



**THIS  
MONTH'S  
FOCUS**

**SECURITY AWARENESS**

**DID YOU KNOW?**

*The most secure hotel rooms are located between the 3<sup>rd</sup> and 5<sup>th</sup> floors, less accessible to the outside but still reachable by emergency services.*

 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**

Glenn Stegall  
*Acting Director*

**Pulse Staff**

Samantha Dambach  
Natalie Perkins  
*Content Developers/Managers*

Isaiah Burwell      Marc Pulliam  
*Content Writer*      *Content Designer*

**SECURITY AWARENESS DURING THE HOLIDAYS**

Security awareness is practiced by DOD and cleared industry personnel all year, however, during the holidays there are several security areas of concern that require increased vigilance due to heightened threats. November and December are months in which online shopping and travel are at their peak, resulting in the need to focus on cybersecurity and travel security.

Organizations can provide reminders and tips to their workforces of cybersecurity and travel threats and how to reduce and avoid them. Individuals can review and refresh their security awareness knowledge prior to shopping online and/or departing for a holiday trip. The Center for Development of Security Excellence (CDSE), the Defense Information Systems Agency (DISA), the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Trade Commission (FTC), and the State Department offer security awareness training/resources for cybersecurity and/or travel security.

**CYBERSECURITY AWARENESS REFRESHER FOR THE HOLIDAYS**

During the holiday season, millions of Americans will be online shopping for great deals. Cyber criminals will also be online targeting online shoppers using fake websites, fake charities, and malicious links. They want access to your personal and financial information to corrupt your data,

plant malicious software on your devices, and steal your identity/money.

CISA advises to use these four methods to protect yourself online:

- Enable multi-factor authentication (MFA) on all accounts.
- Update your software – automatic updates are ideal.
- Think for before you click links – most cyber-attacks start with phishing emails.
- Use strong passwords – a password manager can generate and store unique passwords.



The American Automobile Association (AAA) estimates that in 2023, 115.2 million people will travel between December 23 and January 2.



CISA also offers three **holiday online shopping tips**, which come in the form of downloadable PDFs and videos. The tips are as follows:

- Check Your Devices
- Shop Only Through Trusted Sources
- Use Safe Methods for Purchasing

Check out these tips for detailed guidance on how to implement each tip for a safer online shopping experience. CDSE also offers training courses, videos, webinars, shorts, and posters to inform and refresh users concerning cybersecurity best practices. The Cybersecurity toolkit Training/Awareness tab contains many of the resources organizations and individuals can use to enhance their cybersecurity skills and knowledge to stay safe online at work and home.

The FTC provides information for consumers about safely shopping online, avoiding identity theft, online privacy/

The FTC released a consumer alert on December 6, 2023, notifying the public that scammers have been hiding harmful links in QR codes.

security, protecting kids online, and scams. You can sign up for consumer alerts for current updates sent to your inbox. The website also lists steps to take to report fraud/scams and mitigate identity theft.

It has been reported that scammers have covered parking meter QR codes with their own codes and send codes via text or email with a reason to scan it. Some of the reasons include:

- Information is requested to deliver a package.
- There is a problem with your account and confirmation of information is requested.
- Suspicious activity is reported and to change your password.

Take the following steps to protect yourself from QR scams:

- Inspect QR codes located in unexpected places, checking to see if it is spoofed (misspelled words/switched letter).
- Protect your phone and online accounts with strong passwords and multi-factor authentication.
- Don't scan a QR code in an email or text message you were not expecting.





## MAINTAINING SECURITY AWARENESS DURING TRAVEL

If you are planning to travel during the holidays, don't forget the importance of being vigilant with regards to the security risks. DOD and cleared contractor personnel face the same risk of being the target of criminals as other travelers. They are also prime targets of Foreign Intelligence Services and terrorists. If you are traveling overseas for work or vacation, check with your security office regarding the requirement to receive a foreign travel brief prior to leaving. Security professionals should inform their personnel about travel risks, how to reduce the risks, and steps to take if an incident arises. Individuals should include travel security refresher training in their travel preparations. At a minimum, learn about potential threats, how to reduce your risks, and actions to take in the event a security event happens while traveling. CDSE, the National Counterintelligence and Security Center (NCSC), and the U.S. State Department all offer resources to support

organizational awareness campaigns and individual's knowledge enhancement/refresher. Visit the [July 2023 Pulse](#) for more information on travel security awareness and resources.

Another key resource for domestic and foreign travel is the Antiterrorism Level 1 training. The training contains many useful tips that applies to personal and work travel. Key topics include:

- Air Travel
- Ground Travel
- Hotel Security
- Vehicle Security
- Residence Security

Reviewing these training modules can provide many useful tips to reduce your security risks and ensure safe work or personal travels.

### SECURITY AWARENESS INFORMATION AND RESOURCES (CDSE/DISA/CISA/FTC)

PRODUCT	AGENCY
<a href="#">Holiday Online Safety Tips</a>	CISA
<a href="#">Avoiding Social Engineering and Phishing Attacks</a>	CISA
<a href="#">Preventing and Responding to Identity Theft</a>	CISA
<a href="#">Consumer Advice</a>	FTC
<a href="#">Online Theft and Online Security</a>	FTC
<a href="#">Cybersecurity Awareness Challenge</a>	DISA (Hosted on CDSE Learning Management System)
<a href="#">Phishing and Social Engineering: Virtual Communication Awareness Training</a>	DISA (Hosted on CDSE Learning Management System)
<a href="#">Cybersecurity Toolkit (Training and Awareness Tab)</a>	CDSE
<a href="#">Avoid Scams When You Travel</a>	FTC

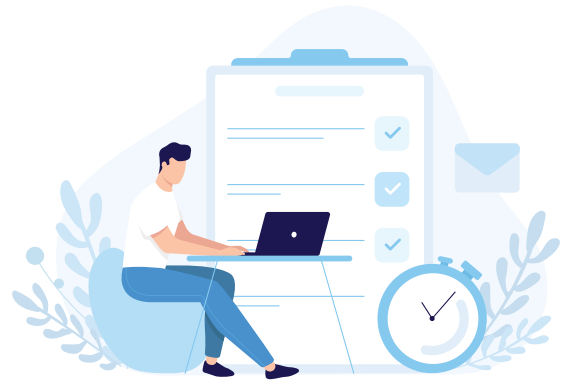


## NEW CDSE EDUCATION COURSES

CDSE is now offering two eight-week virtual instructor-led education courses, *ED202 Writing and Communication Skills in the Security Environment* and *ED203 Writing Incident Reports and Research Papers for DOD Security*. The ED202 course introduces students to the fundamentals of Department of Defense writing and presentation, and the ED203 course prepares students to write security incidents reports and research reports on security-related topics.

The ED202 and ED203 courses replace the ED201 course which was in a 16-week format. Redesigning the ED201 course into two eight-week courses

provides the student more flexibility in scheduling and balancing their work, school and homelife responsibilities. The ED202 course will be offered each Fall Semester in August and ED203 will be offered each Spring Semester in January. CDSE Education courses are delivered on the CDSE's Security Training, Education and Professionalization Portal (STEPP) in our Collaborative Learning Environment virtual classrooms by experienced instructors. While we recommend students take the ED202 course first, it is not a prerequisite for ED203. Both courses are open to all



U.S. Government civilian employees and US military service members with or without a college degree. Upon completing either of these courses, students will earn Professional Development Units (PDUs) that can be used toward maintaining their SP&D Certification. To learn more about these courses and other CDSE Education courses click [here](#).

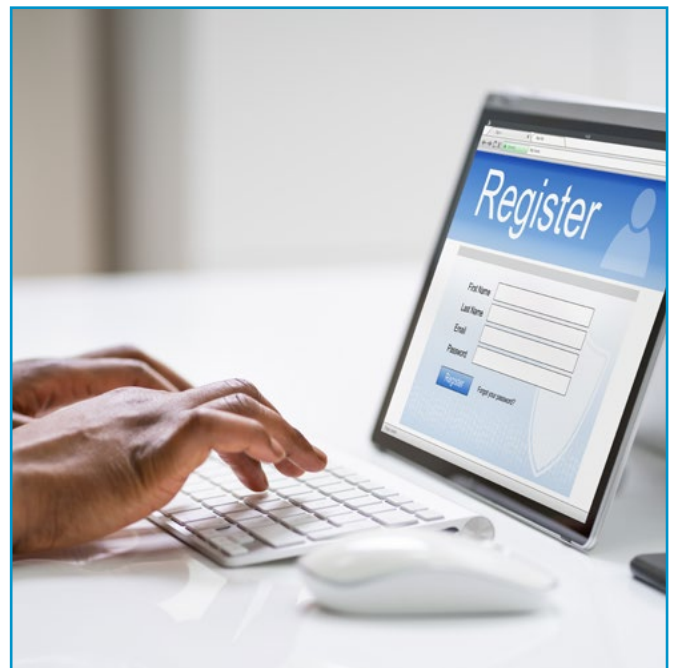
## EDUCATION SPRING SEMESTER REGISTRATION NOW AVAILABLE

The CDSE Education Program Spring 2024 Semester registration is now open! The spring semester classes will run from January 22 to May 19, 2024. Classes fill quickly, so please register early to secure your spot in the spring semester.

CDSE Education Division offers:

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

You can learn more about the classes being offered and register for them by accessing the [course webpage](#). To register, log into [STEPP](#). If you have any questions, or need additional information, contact the [CDSE Education Program](#).







## INSIDER THREAT VIGILANCE CAMPAIGN

The December Vigilance Campaign focuses on reporting. “Supporting Through Reporting” is the central idea behind the campaign, emphasizing that reporting concerning behaviors and risk indicators of coworkers, although uncomfortable, is crucial for the safety of the insider and other colleagues. Previously, reporting had a negative stigma, but it is necessary to prevent and mitigate internal threats.

Training and communication efforts should help all employees understand the spectrum of behaviors to be aware of, how stress can contribute to possible threats, and how to identify and resolve early conflicts or issues. Elevating concerning behaviors and potential risk indicators might require threat assessment and management support.

Proactive measures taken by Insider Threat programs require a multi-disciplinary approach to detect, deter, and mitigate insider threats to organizations.

Please refer to this [additional resource](#).

---

## INSIDER THREAT DETECTION ANALYSIS COURSE (ITDAC) COMING TO CDSE

The ITDAC will be transferring to CDSE in spring 2024. This no cost course is offered to all Executive Branch departments and agencies and is designed for all federal insider threat program analysts from the Department of Defense (DOD), Intelligence Community (IC), and Non-Title 50 (NT-50) communities.

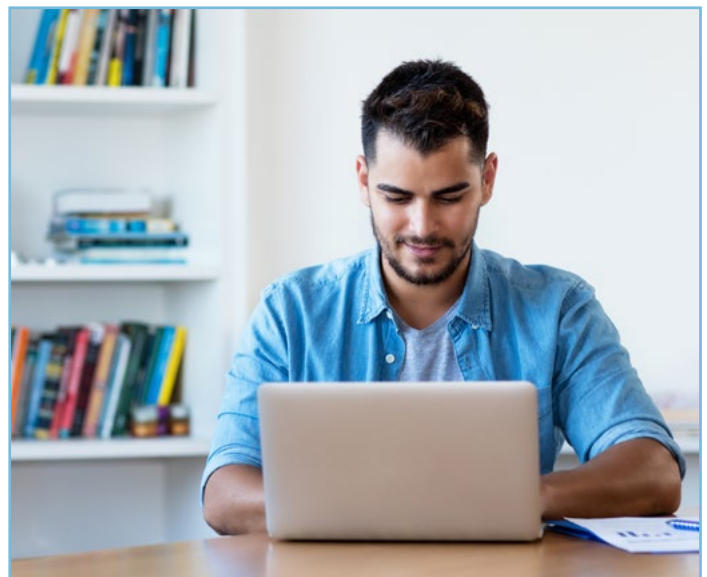
Specifically, this course provides entry level Counter-Insider Threat Analysts the ability to apply critical thinking skills and applicable structured analytic techniques to potential insider threat indicators as learners obtain and use holistic data in conjunction with the application of critical pathway theory. Participants will apply Executive Order, Department of Defense, and IC authorities to gather this holistic data while they ensure constitutional and privacy rights are maintained. Participants will execute the appropriate processes for conducting and reporting insider threat response actions from intake of an initial potential threat to mitigation of the threat. Additionally, students will be able to disclose mandated counterintelligence and criminal activity information to the appropriate agency/office.

Prospective students will need to complete one of two designated tracks within the Insider Threat Program curricula before registering for the ITDAC. For more information, see:

[Insider Threat Program Operations Personnel Curriculum INT311.CU](#)

[Insider Threat Program Management Personnel Curriculum INT312.CU](#)

Registration for the ITDAC will be available soon. Visit [CDSE Insider Threat](#) for more information.



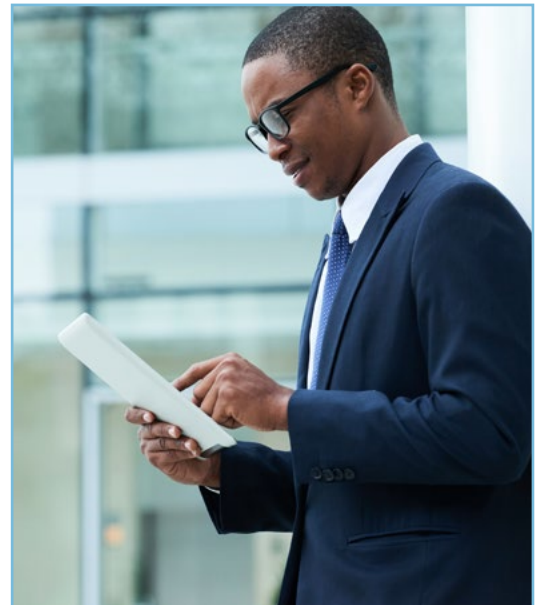


## SIGN UP FOR THE BTAC BULLETIN

The BTAC Bulletin is produced by the DOD Insider Threat Management and Analysis Center's (DITMACs) Behavioral Threat Analysis Center (BTAC) on a monthly basis and responds to observed Insider Threat trends. The BTAC is a multidisciplinary team composed of experts in Threat Assessment/Threat Management, Law Enforcement, Counterintelligence, Behavioral Science, Employee Management Relations, and Cybersecurity. The newsletter offers timely and relevant Insider Threat guidance on applicable issues and contains links and references to research and publications.

### November's Topic - Disgruntlement

Please sign-up and share the newsletter with your government and industry contacts and encourage them to sign-up to receive the BTAC Bulletin and other updates by contacting the BTAC at: [dcsa.quantico.dcsa.list.ditmac-sme@mail.mil](mailto:dcsa.quantico.dcsa.list.ditmac-sme@mail.mil).



## SAVE THE DATE FOR UPCOMING INDUSTRY CONFERENCE

Mark your calendars for the 2024 DCSA Virtual Security Conference for Industry from February 28 to 29, 2024! The conference is open to cleared industry under the National Industrial Security Program (NISP). Stay tuned for more details.

## UPCOMING WEBINAR

Sign up for the following upcoming live webinars:

### **Social Engineering: The Manipulated Insider**

January 11, 2024

12:00 pm to 1:30 pm ET

### **Safeguarding Science: Addressing the Convergence of Emerging Technologies**

January 18, 2024







1:00 pm to 2:30 pm ET

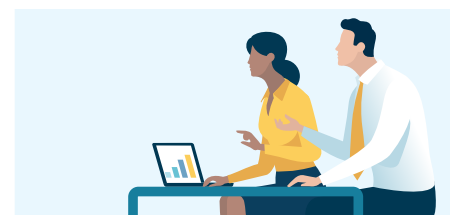
Visit CDSE's [webinar webpage](#) to register for these events and join the discussion!



## FY 2024 UPCOMING COURSES

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 January 2024 to April 2024.

COURSE	DATE	DESCRIPTION
Physical Security and Asset Protection	<a href="#">Mar. 25 - Apr. 14, 2024</a> (VILT) <a href="#">Apr. 29 - May 3, 2024</a> (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	<a href="#">April 16 - 19, 2024</a> (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	 <a href="#">Jan. 8 - Feb. 4, 2024</a> (VILT)  <a href="#">Jan. 9 - 18, 2024</a> (ILT) <a href="#">Feb. 6 - 14, 2024</a> (ILT) <a href="#">Mar. 5 - 13, 2024</a> (ILT)	This course provides students a baseline knowledge to perform common DOD security tasks and practices.
Introduction to Special Access Programs	 <a href="#">March 5 - 8, 2024</a> (ILT)  <a href="#">March 12 - 15, 2024</a> (ILT) <a href="#">April 1 - 9, 2024</a> (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	 <a href="#">Mar. 18 - 22, 2024</a> (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 (ILT)	 <a href="#">Feb. 21 - 22, 2024</a> (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**

**ED502.10 ORGANIZATIONAL CONSIDERATIONS IN APPLYING SECURITY WITHIN THE FEDERAL AND DOD BUREAUCRACY:**

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

“This course helped me to understand the system balance so work can be done without jeopardizing information security.”

“I received more than I expected out of the Security Systems and Cybersecurity course, thanks to the amazing instructor.”

“The instructor was outstanding. She made sure to let me know I was on the right track.”

**ED506.10 HUMAN RESOURCE MANAGEMENT FOR DOD SECURITY:**

“I have a further understanding of the importance of HRM and how it can relate to my profession as a security professional.”

“I learned more about how performance management processes work.”

“I learned requirements (legal) inherent in the HR process and see correlations to security from this course.”

**SEEKING INPUT FOR NEW JOB AID**

We here at CDSE are creating a printable/customizable prohibited personal electronic device (PED) job aid that can be utilized for secure areas (e.g., Special Access Program Facilities and Sensitive Compartmented Information Facilities). What are a few of the top PEDs and/or odd items of concern you would like to see included on this job aid? Send your input to [dcsa.cdsetraining@mail.mil](mailto:dcsa.cdsetraining@mail.mil) using the Subject: New PED Job Aid Input.



**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**

