

New Products (First Quarter FY22)

Background

The Center for Development of Security Excellence (CDSE) is a nationally accredited, award-winning directorate within the Defense Counterintelligence and Security Agency. CDSE provides security education, training, and certification products and services to a broad audience supporting the protection of national security and professionalization of the Department of Defense (DOD) security enterprise.



CDSE Content Areas: Counterintelligence, Cybersecurity, General Security, Industrial Security, Information Security, Insider Threat, Operations Security, Personnel Security, Physical Security, and Special Access Programs

Highlight Summary

CDSE provides courses and products that keep pace with changing policies and evolving security environments. During the first quarter of FY22, CDSE released the following:

- **New Courses:** Cybersecurity, Special Access Programs
- **New Security Shorts:** Physical Security, Counterintelligence
- **New Security Awareness Games:** Cybersecurity
- **New Webinars:** Cybersecurity
- **New Job Aids:** Special Access Programs, Insider Threat, Industrial Security
- **New Case Studies:** Insider Threat

NEW!!

Training Products



Courses

Training to keep security professionals updated on security policy and procedures, delivered online or in-person.

- **Assessing Risk and Applying Security Controls to NISP Systems**
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).
<https://www.cdse.edu/Training/Instructor-led/CS301/>
- **The Special Access Program Personnel Security Official (SPO) eLearning**
This course provides DOD military, civilian, and DOD contractors who perform the duties of a SPO the knowledge required to engage in the Special Access Program (SAP) Nomination process as outlined in DODM 5205.07 Volume 2, Personnel Security.
<https://www.cdse.edu/Training/eLearning/SA106/>



Security Shorts

Allow security professionals to refresh their knowledge of a critical topic or quickly access information needed to complete a job.

- **Functions of Entry Control Facilities (ECFs)/Access Control Points (ACPs)**
This short explains the function of the four ECF/ACP zones: approach, access control, response, and safety.
<https://securityawareness.usalearning.gov/cdse/multimedia/shorts/ecf/story.html>
- **How to Conduct an Inspection – Helpful Tips**
This short provides tips on the formal DOD inspections process to include pre-inspection, inspection, post inspection, and follow-up.
<https://securityawareness.usalearning.gov/cdse/multimedia/shorts/inspection/story.html>
- **Academic Solicitation**
This short enables the workforce to identify academic solicitation methods, determine countermeasures, and report suspicious activity.
<https://securityawareness.usalearning.gov/cdse/multimedia/shorts/academic-solicitation/story.html>
- **Counterintelligence Concerns for National Security Adjudicators**
This short addresses counterintelligence concerns for adjudicators and explains concerns that may affect national security determinations. Individuals who will be involved in evaluating suspected security violations and determinations of eligibility revocation or suspension should clearly understand the counterintelligence concerns for adjudicators.
<https://securityawareness.usalearning.gov/cdse/multimedia/shorts/ci-adjudicator/story.html>
- **Protecting Microelectronics**
This short considers what microelectronics are, DOD microelectronic needs, existing threats, vulnerabilities, and associated reporting requirements.
<https://securityawareness.usalearning.gov/cdse/multimedia/shorts/microelectronics/story.html>
- **Talking with Academia About Security**
This short informs Research Security, Facility Security Officers (FSOs), Counterintelligence Special Agents (CISAs), and other security personnel working with scientists, engineers, and others within cleared academia about the unique challenges of talking to academics about security.
<https://securityawareness.usalearning.gov/cdse/multimedia/shorts/academia/story.html>



Security Awareness Games

Quick and easy ways to test your knowledge and encourage security awareness at your organization.

- **Cybersecurity Magic 8 Ball**
This awareness game is designed to promote cybersecurity awareness as part of National Cybersecurity Awareness Month (NCSAM).
<https://www.cdse.edu/Training/Security-Awareness-Games/>



Webinars

A series of recorded, live web events that address topics and issues of interest to defense security professionals.

- **Cybersecurity and Telework: Concerns, Challenges, and Practical Solutions Pt 3. Collaboration Tools**

This webcast increases awareness of current cybersecurity concerns, challenges, and practical solutions related to the use of collaborative tools while teleworking in the midst of the COVID-19 pandemic.

<https://www.cdse.edu/Training/Webinars-and-Conferences/>



Job Aids

Security products designed to provide guidance and information to perform specific tasks

- **SAP Nomination Process (SAPNP)**

This job aid reinforces the responsibilities and procedures for the SAP Nomination Process. It is suitable for viewing online and also can be printed as a handy desk reference.

<https://www.cdse.edu/Portals/124/Documents/jobaids/sap/sapnp-quick-ref-aid.pdf?ver=ZD0uUSbsU0AXHVZnom1Sng%3d%3d>

- **2022 Insider Threat Vigilance Campaign**

This job aid is a vigilance campaign that helps implement Insider Threat Awareness training. Vigilance campaigns are loaded with awareness resources to share within an organization. Use what we have created for 2022 to jump-start your annual campaign.

<https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTVigilanceCampaign.pdf>

- **Potential Risk Indicators: Insider Threat**

Most insider threats exhibit risky behavior prior to committing negative workplace events. If identified early, many risks can be mitigated before harm to the organization occurs. This job aid provides information on insider threat potential risk indicators. It has been updated to align with national security adjudicative guidelines.

<https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf>

- **Industrial Security Program Annual Planner**

This job aid serves as a supplemental tool to help support and grow industrial security training and awareness within your organization. It is a combination of performance support tools selected from various security content areas that comprise the industrial security discipline that you can utilize to promote security awareness throughout the year on a monthly basis.

<https://www.cdse.edu/Portals/124/Documents/jobaids/industrial/Industrial-Security-Program-Annual-Planner.pdf>



Case Studies

Analyzed accounts of real-world security activities, events, or threats.

- **Glen Omar Viau Case Study**

This Case Study on Miriam Taha Thompson for unauthorized use of government property and falsifying facts covers the crime, sentence, impact, and potential risk indicators in a case of espionage.

<https://securityawareness.usalearning.gov/cdse/case-studies/index.php>

- **Wei Sun Case Study**

This Case Study on Wei Sun for insider and export violations covers the crime, sentence, impact, and potential risk indicators in a case of espionage.

<https://securityawareness.usalearning.gov/cdse/case-studies/index.php>

- **Azzam Mohamed Rahim Case Study**

This Case Study on Azzam Mohamed Rahim for the attempt to provide material support to a foreign terrorist organization covers the crime, sentence, impact, and potential risk indicators in a case of espionage.

<https://securityawareness.usalearning.gov/cdse/case-studies/index.php>

- **Jesus Encarnacion and Jarrett William Smith Case Studies**

Case Studies on Jesus Encarnacion and Jarrett William Smith demonstrate indicators and the impact of individuals guilty of aiding terror groups.

<https://securityawareness.usalearning.gov/cdse/case-studies/index.php>

- **Richard Liriano Case Study**

This Case Study on Richard Liriano for cyber-threats covers the crime, sentence, impact, and potential risk indicators in a case of espionage.

<https://securityawareness.usalearning.gov/cdse/case-studies/index.php>

- **Randall Hughes Case Study**

This Case Study on Randall Hughes for kinetic violence covers the crime, sentence, impact, and potential risk indicators in a case of espionage.

<https://securityawareness.usalearning.gov/cdse/case-studies/index.php>

- **Izaak Kemp Case Study**

This Case Study on Izaak Kemp for mishandling classified information covers the crime, sentence, impact, and potential risk indicators in a case of espionage.

<https://securityawareness.usalearning.gov/cdse/case-studies/index.php>