CDSE pulse
VOLUME 4 ISSUE 3
March 2023

THIS MONTH'S FOCUS

HANDLING CLASSIFIED INFORMATION

DID YOU KNOW?

In 1951 President Truman issued E.O. 10290 which established the first umbrella program to protect classified information for all departments and agencies of the Executive Branch.

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

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

HANDLING CLASSIFIED INFORMATION

When it comes to classified information that is vital to national security, there are specific rules for how to handle it. The DOD Information Security Program establishes policy guidance for classifying, protecting, sharing, downgrading, declassifying, and destroying classified. This article will give an overview of safeguarding, disseminating, and destroying classified information.

SAFEGUARDING

Safeguarding refers to using prescribed measures and controls to protect classified information. The first safeguarding measure is ensuring that only authorized personnel have access to classified information. The three requirements for individual access to classified information are national security eligibility, a need-to-know the information, and a completed Standard Form (SF) 312, Classified Information Nondisclosure Agreement.

There also must be established access control measures, which detect and deter unauthorized access. These security countermeasures can include fences, badges, guards, security containers, locks, intrusion detection systems, and other countermeasures. For more information on access control measures, visit the **Physical Security Toolkit**.

Where are you authorized to safeguard classified information?:

- An authorized individual's possession
- Approved secure room/ secured open storage
- A General Services Administration (GSA) approved security container
- Authorized information technology (i.e. classified IT system)

Classified information in an authorized person's head or hands cannot be disclosed to another individual unless they meet the three criteria mentioned earlier. When hand-carrying classified information, the individual should use a classified document cover sheet (SF-703 - Top Secret/ SF-704 – Secret/SF-705 – Confidential). This is to alert holders to the presence of classified information and to prevent the viewing of classified information by unauthorized personnel.

When not directly in an authorized individual's possession, classified information must be stored in a GSA-approved security container such as a two or four drawer cabinet, a safe, or a vault. View the **Classified Storage Requirements Short** to assist with identifying the appropriate storage requirements for different types and levels of classified information. All locks for GSA-approved security containers must conform to Federal Specification FF-L2740. Visit the CDSE Physical Security Job Aids and Physical Security Training Videos webpages for information

and demonstrations on operating the different GSA approved security container locks.

Activity Security Forms:

- SF-700, Security Container Information
- SF-701, Activity Security Checklist
- SF-702, Security Container Check Sheet
- CDSE has Information Security Shorts for each of these forms

When using information technology to access classified information, users must follow cybersecurity policies related to accessing or sharing classified information on classified systems such as the Secure Internet Protocol Router Network (SIPRNET).

DISSEMINATION

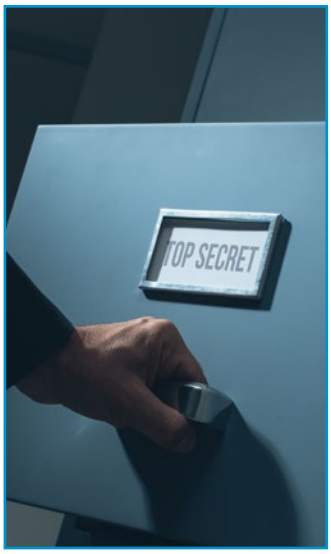
Dissemination refers to the sharing or transmitting of classified information to others who have authorized access to that information. Some of the methods include transmission, transportation, and classified meetings. Transmission is the act of sharing classified information via a phone, information system, or fax. Those sharing classified information with authorized individuals via the phone must use approved Secure Terminal Equipment (STE). Individuals who use STE must be vigilant about their surroundings to ensure no one can overhear their conversation.

Transmitting classified information via an information system can give rise to difficult security issues. Only use an information system that has been specifically authorized to process classified information and only email classified information over a classified network. When faxing classified information, there are several conditions that must be met. The fax machine must be connected using secure communications equipment and circuits which are approved for transmission of information at the specific level of classification.

Transporting classified information requirements vary based upon the level of classification. The more sensitive the information the more restrictions there are. The primary factor you need to consider when selecting a method is the classification level of the information you need to move (Confidential, Secret Top Secret). There are also special types of information that have special controls on dissemination. Access the CDSE job aid, Transmission and Transportation for DOD: Dissemination of Special Types of Information to learn more. Classified information can be transported via hand-carrying or an escort, courier, or mail. Download a copy of the Transmission and Transportation Authorized Methods by Classification Level job aid for quick reference.

There are special rules for wrapping and packaging classified material to reduce the risk of loss or compromise during transporting. DoDM 5200.01, Volume 3 outlines the mandatory baseline policies and procedures to protect classified information during transportation. Additionally, the DOD components are responsible for establishing procedures for transmission and transportation of classified information reduce the risk of compromise while permitting use of the most cost-effective means. View CDSE's **Packaging Classified Documents Video** for step-by-step instructions.

For a classified meeting or conference, the sponsoring DOD activity will assign an official to act as the security manager for the event. The security manager is responsible for multiple security provisions, including briefing attendees on safeguarding



procedures, controlling the entrance so that only authorized personnel gain entry to the area, and controlling the perimeter to ensure unauthorized personnel cannot overhear classified discussions or introduce prohibited devices. View the CDSE **Classified Meetings and Conferences Short** to learn more about the procedures to follow and related potential security risks.

DESTRUCTION

The last step in the Information Security Program life cycle is destruction. Destruction refers to destroying classified information so that it cannot be recognized or reconstructed. Authorized methods for destroying classified information include burning, shredding, pulverizing, disintegrating, wet pulping, melting, chemical

decomposition, and mutilation. Destruction of classified information must be done on approved equipment. The National Security Agency (NSA) maintains an **evaluated products lists (EPL)**, which contain destruction products that have been tested and meet performance requirements. The NSA EPL also contains a list of approved devices to destroy optical media devices such as compact and digital video disks. Other storage media such as thumb drives, zip disks, or computers should be destroyed in coordination with local, approved methods. View the Disposal and Destruction of Classified Information Short for more information.

In conclusion, classified information must be protected in every step of its life cycle to protect national security. Properly safeguarding, disseminating, and destroying classified information are important components of an effective information security program. Understanding requirements and procedures is a shared responsibility for individuals and security personnel within DOD. CDSE information security training and resources are available all year round to support the DOD workforce in protecting classified information.

INFORMATION SECURITY RESOURCES

PRODUCT	URL
Introduction to Information Security (eLearning)	https://www.cdse.edu/Training/eLearning/IF011/
Transmission and Transportation for DOD IF107.16 (eLearning)	https://www.cdse.edu/Training/eLearning/IF107/
Dissemination of Classified Information Within and Outside of the Executive Branch (Job Aid)	https://www.cdse.edu/Portals/124/Documents/jobaids/information/Classification_Trifold_Final.pdf
Packaging Classified Documents (Video)	https://www.cdse.edu/Training/Security-Training-Videos/Information/Packaging-Classified-Documents/
Classified Storage Requirements (Short)	https://securityawareness.usalearning.gov/cdse/multimedia/shorts/csr/story_html5.html
Classified Meeting and Conferences (Short)	https://securityawareness.usalearning.gov/cdse/multimedia/shorts/classified/story.html
NATO Information (Short)	https://securityawareness.usalearning.gov/cdse/multimedia/shorts/nato/story_html5.html
Disposal and Destruction of Classified Information (Short)	https://securityawareness.usalearning.gov/cdse/multimedia/shorts/dnd/story_html5.html
Tabs: Transmission/Transportation & Protection/Handling (Toolkit)	https://www.cdse.edu/Training/Toolkits/Information-Security-Toolkit/
NSA Evaluated Products Lists	https://www.nsa.gov/Resources/Media-Destruction-Guidance/

SPECIAL PROGRAM SECURITY CREDENTIAL (SPSC)

The Security Professional Education Development (SPēD) Program's Special Program Security Credential (SPSC) is now live!

Formerly a certification, this credential is intended for candidates who currently hold a Security Fundamentals Professional Certification (SFPC), and:

- Perform (or will be performing) Security Officer functions for or on behalf of the DOD Special Access Program (SAP) or
- Are working toward or already occupy a full time security position for which attainment of this credential has been deemed a requirement or professional development milestone

For more information regarding the SPSC, as well as scheduling your assessment, refer to your Component Service Representative, **https://www.cdse.edu/Certification/Additional-Certification-Credential-Assistance/**.

NEW INSIDER THREAT JOB AID

CDSE recently released the Insider Threat Fraud job aid. This job aid provides information relating to fraud and its relevance to insider threat. This product provides information that is useful to the counter-insider threat practitioner, organizational members and leaders in countering the risk of fraud perpetrated by insiders with trusted access. Access the new **job aid** today!

NEW PRODUCTS FROM THE THREAT LAB NOW AVAILABLE

The Defense Personnel and Security Research Center (PERSEREC) produces the Bottom Line Up Front (BLUF) products that highlight what The Threat Lab personnel are watching, listening to, reading and thinking about. Issue 8 artifacts, which focus on Critical Thinking and Issue 9 artifacts, which focus on Bystander Effect, are now available in the Research Tab of the Insider Threat Toolkit. Visit **https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/#research** to check out the latest and previous issues of the BLUF.

SAVE THE DATE: 2023 VDSCI

Mark your calendars for the virtual DCSA Security Conference for Industry (vDSCI), scheduled for April 26-27, 2023. Stay tuned for more information by subscribing to the Flash, Pulse, or checking the Webinars and Conferences **webpage**.

UPCOMING ILT/VILT TRAINING 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 (SPēD) Program certifications and credentials, and select courses have ACE CREDIT recommendations that may earn transfer credits at participating universities. Below is a list of ILT/VILT courses available May - June 2023. The full FY23 schedule can be found **here**.

Physical Security and Asset Protection (ILT)

May 1 – 5, 2023 (ILT)

This course provides students the information needed to identify and utilize regulatory guidance, methodologies, and concepts for protecting DOD assets. Students will learn how to apply the risk management process, conduct problem solving, and incorporate best practices to develop courses of action utilizing physical security measures, based on a cost-benefit analysis, to protect an installation's assets.

Getting Started Seminar (GSS) for FSOs (VILT)

May 2 – 5, 2023

This course is not only a great way to get started as a new Facility Security Officer (FSO), but also a way for experienced FSOs to learn about policy changes, procedural changes, emerging trends, threats, concerns, etc. Students work in collaboration with other security professionals, exploring security topics through practical exercises.

DOD Security Specialist Course (VILT)

May 22 – June 18, 2023

This course provides students a baseline of fundamental knowledge to perform common DOD security tasks and practices. It incorporates industrial, information, personnel, and physical security disciplines to understand their interrelationships, related policies, programs, and procedures.

Assessing Risk and Applying Security Controls to NISP Systems (ILT)

June 5 – 9, 2023

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).

DOD Security Specialist Course (ILT)

June 21 – 29, 2023

This course provides students a baseline of fundamental knowledge to perform common DOD security tasks and practices. It incorporates industrial, information, personnel, and physical security disciplines to understand their interrelationships, related policies, programs, and procedures.

REGISTER FOR GSS COURSE AT THE NCMS ANNUAL SEMINAR

CDSE will be hosting the Getting Started Seminar (GSS) for New Facility Security Officers (FSOs) course at the NCMS Annual Training Seminar on June 5, 2023! This course is not only a great way to get started as a new FSO, but also a way for experienced FSOs to keep informed of policy changes, procedural changes, and emerging trends and concerns. Students work in collaboration with other security professionals, exploring security topics through practical exercises. Topics include the DD 254, insider threat, reporting requirements, counterintelligence, security and contractor reviews, security training and briefings, and personnel security.

Please pre-register and complete the pre-requisites at **https://www.cdse.edu/Training/Instructor-led/IS121/**. Registration closes on May 15, 2023, and only registered participants will be allowed to attend. Proof of registration (emailed by CDSE) and a photo ID will be required for class entry.

WHAT THE SECURITY COMMUNITY IS SAYING

Derivative Classification (IF103.16) | eLearning:

"As someone who sometimes goes years without working with classified information, this is an excellent refresher course. Good narrator, very good scenarios at the end."

"Of all the training I've had that covered this subject, this was the easiest to follow and made the most sense."

"Excellent online course with current and relevant reference materials and scenarios."

CDSE LINKEDIN

Did you know that CDSE is now on **LinkedIn**? Follow our profile for real-time information on professional development opportunities such as courses and events!

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 - **https://www.cdse.edu/news/index.html**.

Insider Threat Bulletins	Weekly Flash	Quarterly Product Update