CDSE pulse
VOLUME 3 ISSUE 6
June 2022

THIS MONTH'S FOCUS

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

DID YOU KNOW?

Limited Dissemination Control (LDC) markings are used to limit and/or control who can or cannot access CUI based on a specific law, regulation, or policy.

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

Zinethia Clemmons
Chief, Shared Services

Pulse Staff

Adriene Brown
Chief Content Officer

Samantha Dambach

Natalie Perkins
Content Developers/ Managers

Isaiah Burwell
Content Writer

Marc Pulliam
Content Designer

THE HISTORY AND IMPORTANCE OF CUI

Controlled Unclassified Information (CUI) is unclassified information that requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies. The CUI program has been an unprecedented initiative, standardizing practices across more than 100 separate departments and agencies to enable timely and consistent information sharing. This initiative also aims to increase transparency throughout the Federal Government and with non-federal stakeholders.

Sharing CUI is authorized for any activity, mission, function, operation, or endeavor that the U.S. Government authorizes. CUI provides a uniform marking system across the Federal Government that replaces a variety of agency-specific markings, such as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive but Unclassified (SBU), etc.

The concept for CUI began in 2004 when the 9/11 Commission Report recommended the horizontal sharing of intelligence information, transcending individual agencies. Executive Order (EO) 13556 established a comprehensive CUI program in November 2010. It designated the National Archives and Records Administration (NARA) to serve as the Executive Agent (EA) to implement and oversee agency actions to ensure compliance with the EO.

As stated in the Title 32 CFR, CUI can be as follows:

- Information the Government creates or possesses;
- Information another entity creates or possesses on behalf of the Government.

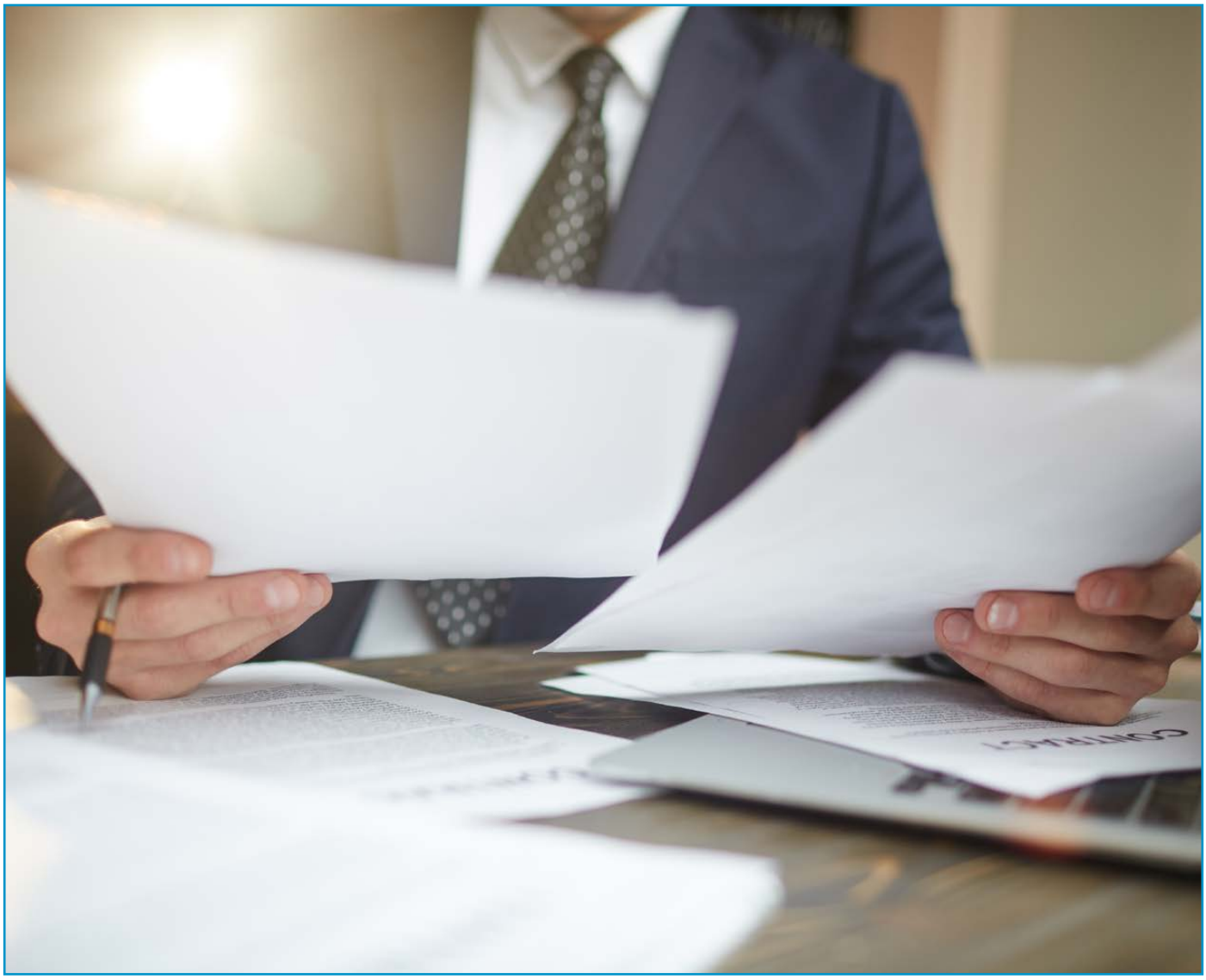
For example, the Government creates work products and emails while information associated with contracts is created on behalf of the Government. In either case, laws, regulations, or Government-wide policies protect CUI information. Other examples of CUI include defense critical infrastructure information, export controlled information, information related to sensitive international agreements, and law enforcement information. Information that does not qualify as CUI is classified, not created by, or not under the control of the U.S. Government such as, a non-executive

On September 14, 2016, **section 2002.4 of Title 32 Code of Federal Regulations (CFR)**, defined CUI as "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls."

branch journal article on counterinsurgency.

CUI is handled, stored, transmitted, and destroyed in a similar manner to the legacy FOUO program. It should be processed on government furnished equipment, encrypted if sent via Non-classified Internet Protocol Router Network (NIPRNet), and only accessible on a limited basis to those with a lawful Government purpose. It must be destroyed by means approved for destroying classified information or in a manner making it unreadable, indecipherable, and irrecoverable. After working hours, CUI can be stored in unlocked containers, desks, or cabinets if the Government building provides security for continuous monitoring of access. If there is no building security, the information must be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas.

Establishing CUI was an impactful moment in DOD's information security program, formally acknowledging that certain types of unclassified information are extremely sensitive, valuable to the United States, sought after by strategic competitors and adversaries, and often have legal safeguarding requirements. Unlike with classified national security information, DOD personnel at all levels of responsibility and across all mission areas receive, handle, create, and disseminate CUI. CUI allows us to create a better, more unified front of protection against those who wish to steal our information and harm our country.



CUI ORGANIZATIONAL ROLES AND RESOURCES

There are several government agencies and organizations that play key roles in the development, implementation, and oversight for DOD and cleared industry CUI programs. These entities create CUI policy, guidance, training, and resources to in support CUI programs. The following organizations offer critical contributions to CUI programs for DOD and cleared industry:

National Archives and Records Administration (NARA)/ Information Security Oversight Office (ISOO). EO 13556, Controlled Unclassified Information designated NARA as the EA to implement and oversee agency actions to ensure compliance with the EO. The Archivist of the United States established the CUI Office within NARA to fulfill the responsibilities of CUI EA and appointed the Director of the Information Security Oversight Office (ISOO) as Director of the CUI Office. As the CUI EA, ISOO issues guidance to Federal agencies on safeguarding and marking CUI. The NARA and ISOO CUI website features the CUI registry, history, policy, guidance, reports, training, FAQs, and resources. Visit the **NARA/ISOO website** to access this wealth of CUI information.

The Controlled Unclassified Information (CUI) blog is an educational and informative resource, run by NARA, to support implementation of the Federal CUI Program. The purpose is to promote a better understanding of the CUI Program and how it works. **Subscribe today!**

Office of the Under Secretary of Defense (OUSD), Intelligence and Security (I&S), Information Security (INFOSEC) Office. In DOD, OUSD(I&S) INFOSEC Office issues policy guidance for the identification and protection of CUI. It promotes information sharing, provides resources, and develops uniform and standardized management processes for implementation of CUI. The OUSD(I&S) INFOSEC Office employs, maintains, and enforces standards for safeguarding, storing, destroying, transmitting, and transporting CUI. It also promotes security education and training for all of DOD. Additionally, the OUSD(I&S) INFOSEC Office mitigates the adverse effects of unauthorized access CUI by investigating and acting upon reports of security violations and compromises of CUI. Visit the **DOD's CUI website** to view the DOD CUI registry policy, training, job aids, and news.

DOD CUI Marking Guide job aid for training on how to properly apply CUI markings. **View it here!**

Defense Counterintelligence and Security Agency (DCSA). DCSA is responsible for overseeing CUI requirements and implementation for cleared contractors in accordance with the National Industrial Security Program (NISP). DOD Instruction 5200.48 assigned DCSA with eight responsibilities related to CUI. DCSA is currently implementing a plan to execute these responsibilities using a phased approach to operationalize its CUI responsibilities throughout the duration of Fiscal Year 2022 (FY22). DCSA's industry CUI website provides more information about the current status of their CUI oversight mission and Phase 1 of the implementation plan. Guidance is also listed for what industry can do now. Additionally, the website provides oversight policy, training requirements, and resources for DOD and industry. Visit the **DCSA CUI website** to view these helpful CUI resources for cleared industry.

The DCSA CUI "Quick Start Guide for Industry" is a good resource for industry CUI personnel get critical information about CUI and how to develop a program. **Find it here!**

Center for Development of Security Excellence (CDSE). CDSE offers CUI training and resources for DOD and cleared industry. The DOD Mandatory Controlled Unclassified (CUI) Training is an eLearning course offered on CDSE's Security Awareness Hub. The course provides information on the 11 training requirements for accessing, marking, safeguarding, decontrolling and destroying CUI along with the procedures for identifying and reporting

security incidents. The course also meets the CUI training requirement for industry when required by Government Contracting Activities for contracts with CUI requirements. Visit the **course page** to learn more and take the training.

The CUI toolkit is CDSE's primary CUI information source. On 1 June, CDSE released the new/revised CUI toolkit. Using a web-based approach, the redesigned toolkit focuses more on user accessibility, enhancing the navigation experience for the customer by making it easier to find and view content. The toolkit provides DOD and industry personnel with easy access to applicable National DOD policy and training guidance, as well as other critical job aids and resource information for CUI. Visit the new **CUI toolkit** today!

2,561,401

As of 1 June, 2022, there have been 2,561, 401 of DOD Mandatory CUI training course completions.

UD COURSE REQUIRED FOR INSIDER THREAT CURRICULA

The Insider Threat Curricula (Insider Threat Program Operations Personnel track and Insider Threat Program Management Personnel track) includes the Unauthorized Disclosure (UD) of Classified Information and Controlled Unclassified Information (CUI) IF130.16 eLearning course. This one-hour eLearning course provides an overview of what unauthorized disclosure is, including specific types of UD, some common misconceptions about UD, the types of damage caused by UD and the various sanctions one could face if caught engaging in UD. It is intended for all collaterally cleared DOD civilian, military, and contractor personnel.

To access and learn more about this course, visit: **https://www.cdse.edu/Training/eLearning/IF130-resources/**

To read about cases of unauthorized disclosures made by insider threats, visit: **https://securityawareness.usalearning.gov/cdse/case-studies/index.php**

UPCOMING WEBINARS

CDSE invites you to join our upcoming webinars:

Disinformation and Insider Threat
Thursday, July 7, 2022
12:00 – 1:00 p.m. ET

Conducting an Effective Self-Inspection
Thursday, July 14, 2022
1:00 p.m. to 2:00 p.m. ET

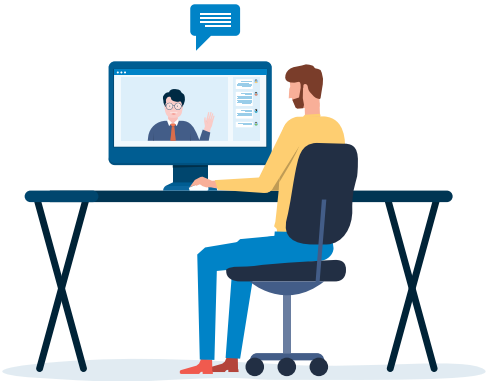
Physical Security Posture: Security-In-Depth
Wednesday, August 31, 2022
12:00 – 1:00 p.m. ET

Counter Insider Threat Resources for Your Organization
Thursday, September 8, 2022
12:00 – 1:00 p.m. ET

Register today for all four events and join the discussion!

NAESOC WEBCAST NOW AVAILABLE

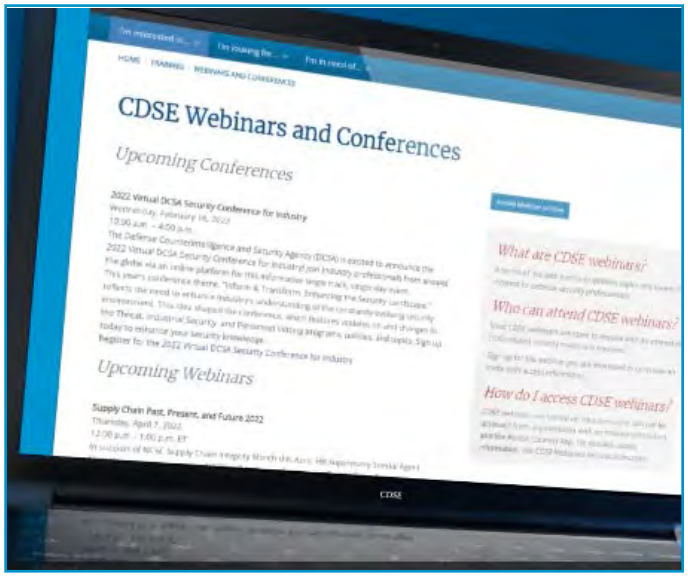
CDSE recently released the "Lessons Learned and Best Practices from the NAESOC" webcast. This webcast is geared towards the Facility Security Officer or Senior Manager at facilities assigned to the National Access Elsewhere Security Oversight Center (NAESOC). It provides strategies and available resources that will assist you in maintaining an effective security program. Access the recording at **https://www.cdse.edu/Training/Webinars-and-Conferences/Webinar-Archive/Lessons-Learned-and-Best-Practices-from-the-NAESOC/**



NEW PSA RELEASED

CDSE has a new Public Service Announcement (PSA) available to share and download on the Defense Visual Information Distribution Service (DVIDS). You can also view all the past PSAs in our **Electronic Library**.

Webinars and Conferences (**https://www.dvidshub.net/video/844735/cdse-webinar-and-conference-psa**)



AUGUST DOD SECURITY SPECIALIST COURSES

The next DOD Security Specialist Course (SSC) is scheduled to start August 1, 2022 and is entirely virtual! The four-week, virtual SSC has been well-received within the community averaging over 85 percent approval rating amongst students. The 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.

To learn more, register, and view the required prerequisites, visit: **https://www.cdse.edu/Training/Virtual-Instructor-led-Courses/GS101/**

INSIDER THREAT SENTRY APP

Have you downloaded the Insider Threat Sentry App? This mobile addition to CDSE's insider threat portfolio expands the availability of posters, videos, security awareness games, job aids, case studies, and more. The application is available for users from the Android and iOS app stores. The app provides direct access to relevant insider threat content in one easy-to-use place. Download it today!

REGISTER FOR FALL EDUCATION CLASSES

Registration is now open for the fall semester of CDSE Education classes that run from August 22 to December 18, 2022. Classes fill quickly, so please register early to secure your spot in the fall semester.

CDSE Education program 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 links located here: **https://www.cdse.edu/Education/Courses/**

To register, log into STEPP via: **https://cdse.usalearning.gov/local/pwt_privacy_policy/view.php**

If you have any questions, or need additional information, send inquiries to: **dcsa.cdseeducation@mail.mil**

UPCOMING SECURITY CONFERENCES

Save the dates for these two 2022 security conferences. Registration is not yet available but will be announced in future Pulse issues, the CDSE Flash, CDSE's social media and on the **CDSE Webinars and Conferences** webpage.

2022 Insider Threat Virtual Security Conference
September 1, 2022

2022 Virtual DOD Security Conference (vDSC)
October 19-20, 2022

WHAT THE SECURITY COMMUNITY IS SAYING

DOD Mandatory CUI Training (IF141.16)

"CUI Implementation is new, this was a very well designed course to cover those concepts."

"I am the first line CUI SME for geospatial products and information for my program. This training is an excellent introduction to CUI as it is not too technical, has excellent flow, and covers the important content."

Unauthorized Disclosure of Classified Information and Controlled Unclassified Information (CUI) (IF130.16)

"Thoroughly enjoyed the animation and speakers. This is the best online course I have taken so far. Easy to learn and navigate. Kept my interest up."

"I have 20 years k-12 teaching experience. This training is by far the best (mandatory requirements) at actually applying and measuring relevant learning concepts. Well done."

VIRTUAL DCSA SECURITY CONFERENCE FOR INDUSTRY RECORDINGS

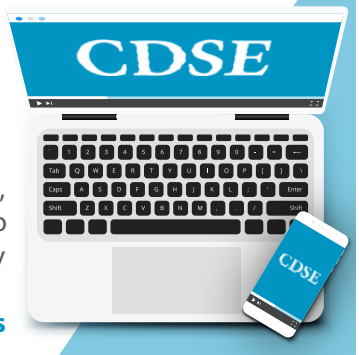
The recordings from February's conference are now available!

If you attended the virtual conference or if you registered but were not able to attend, you have been pre-registered to retrieve the recordings. **Visit https://cdse.acms.com/vdsci22recording/event/login.html** to view anything you may have missed/want to revisit.

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 publications, visit our news page to sign up or update your account today

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



Insider Threat Bulletins	Flash	Quarterly Product Report