

Enterprise Security Operations Controlled Unclassified Information (CUI) Quarterly Newsletter



CUI Updates

- Please note that the Defense Counterintelligence and Security Agency (DCSA) CUI Branch Newsletter will now be published quarterly instead of monthly.
- Thank you to everyone who has already sent in their updated contact details. To ensure you continue to receive important communications, please send any future updates to our CUI Branch Action Officer, Lilian Benitez, at lilian.l.benitez.civ@mail.mil
- The Office of the Chief Information Officer (OCIO) has released Revision 2.2 of the Cybersecurity Maturity Model Certification (CMMC) Program Frequently Asked Questions (FAQs). You can access the document to stay informed on the latest updates here: <https://dowcio.war.gov/Portals/0/Documents/CMMC/CMMC-FAQsv4.pdf>
- Additionally, a wealth of information regarding CMMC is available on their website: <https://dodcio.defense.gov/cmmc/Resources-Documentation/>
- For a comprehensive collection of tools and information, please visit the official DCSA CUI Resources for Industry page at <https://www.dcsa.mil/Industrial-Security/Controlled-Unclassified-Information-CUI/Resources/>

FAQs

- DCSA has noted an increase in questions regarding Facility Clearance (FCL) Verification letters generated from the National Industrial Security System (NISS), which is a system marked as containing CUI. For detailed guidance on Information Safeguarding for FCL Letters, please see the July 2025 edition of the "Voice of Industry" (VOI) newsletter, available on the DCSA website: <https://www.dcsa.mil/Portals/128/Documents/CTP/tools/250731%20VOI%20Newsletter%202.0.pdf>. The core guidance is as follows: To assist Industry with meeting the task of providing FCL letters as part of their Request for Proposal (RFP) process, the following Designator Indicator (DI) block should be added to each FCL letter prior to providing it to the Government Contracting Activity (GCA):

Controlled by: Defense Counterintelligence and Security Agency
Controlled by: Contractor Facility Name (CAGE Code)
CUI Category: OPSEC
LDC: FEDCON
POC: Verification & Triage Unit (VTU) / dcsa.quantico.hq.mbx.occ-facilities@mail.mil

- Another common question received by DCSA relates to the proper handling of internal Personally Identifiable Information (PII). DCSA has published official guidance to address this, which is available in the DCSA CUI FAQs document that can be found here: [https://www.dcsa.mil/Portals/128/Documents/CTP/CUI/DCSA%20CUI%20Frequently%20Asked%20Questions%20\(May%202025\).pdf](https://www.dcsa.mil/Portals/128/Documents/CTP/CUI/DCSA%20CUI%20Frequently%20Asked%20Questions%20(May%202025).pdf). The core guidance is as follows: Personally identifiable information collected on behalf of the company or for the purpose of industry use should be protected in accordance with that company's policy, applicable law, and industry standard. Once the information is transmitted to the government, it will be safeguarded as CUI.

Newsletter Contact Information

Dr. Dennis C. Daniels, Chief, CUI Branch, Enterprise Security Operations, Industrial Security, DCSA
Office: (571) 305-6062, Cell: (571) 660-0970, dennis.c.daniels.civ@mail.mil
CUI Mailbox: dcsa.quantico.ctp.mbx.eso-cui@mail.mil - CUI Hotline: 571-305-4878

Trends

DCSA has observed a recent increase in reports of Unauthorized Disclosures (UD) of information. We would like to provide clarity on the proper procedures and DCSA's role in this process. Please be aware that DCSA's Industrial Security division does not have the authority to conduct inquiries or investigations into these unauthorized disclosures. While we forward all reports to the DCSA Unauthorized Disclosure Program Management Office (UD PMO), their ability to act is limited without specific details. The UD PMO tracks and documents the types of CUI that have been released. However, if reports do not specify the category of CUI involved, it is difficult for any action to be taken. Ultimately, DCSA will share the information received with the relevant Government Contracting Activity (GCA). As the owner of the information, the GCA is the appropriate entity to validate whether the released information is indeed CUI and to determine the next steps. To ensure your report can be addressed effectively, please include the specific category of CUI that was disclosed. This information is critical for the UD PMO's tracking efforts and for the GCA to take appropriate action.

Engagements

Recent Engagements

- The GBS Group (Virtual) – January 27, 2026
- CUI Conference (CUI CON) (Orlando, FL) – February 11 – 13, 2026

DCSA Highlights Its Role in CUI Mission at CUI-CON 2026: DCSA was a key participant in this year's CUI-CON 2026. During the conference, DCSA provided an important update on its role within the CUI mission. The annual conference is specifically designed to assist Department of War (DoW) contractors with implementing CUI safeguarding requirements and preparing for the CMMC to meet their contractual obligations. The photos below capture scenes from CUI-CON 2026.



Photo 1 (Left): Mr. Richard Rayner, a keynote speaker from DCSA, provided an update on DCSA's role within the CUI Mission Space. Photo 2 (Right): Mr. Rayner (right) in conversation with Mr. James Goepel, Executive Vice President and General Counsel of Peak InfoSec LLC, during their fireside chat.

Upcoming Engagements

- DCSA Western Region Industry Day (Honolulu, HI) – March 3, 2026
- NCMS Live (Virtual) – March 5, 2026
- Microchip (Chandler, AZ) – April 8, 2026
- CS5 Conference (San Diego, CA), April 16, 2026
- NCMS Live (Virtual) – May 7, 2026
- DCSA Central Region Industry Day (Virtual) – June 1, 2026
- NCMS 62nd Annual Training Seminar (Atlanta, GA) - June 9, 2026