CDSE Center for Development of Security Excellence

Webinar Questions and Answers

Kicking Off a CUI Awareness Campaign

On August 1, 2024, the live webinar was held. The Q&A below provides answers to the additional questions that were not answered during the live/recorded Q&A portion of the webinar.

1. **Question:** Should we mark our Annual Security Review Binder Materials for DCSA - CUI even though we are not official CUI certified originators?

   Answer: Controlled unclassified information (CUI) certified originators do not exist in the CUI program. CUI is identified, not originated. All DOD personnel (military, civilian, and contractor) are authorized to identify and mark CUI provided they have taken the mandatory DOD CUI training.

2. **Question:** Isn't it dangerous to send any CUI or sensitive data on any iPhone or computer as AI is dangerous? Ref: Weaponization of AI webinar?

   Answer: As a best practice, avoid wireless telephone transmission of CUI when other options are available. CUI should only be sent on systems that meet National Institute of Standards and Technology (NIST) 800-171 and 800-53 standards for federal and non-federal systems.

3. **Question:** Can MS teams be used to maintain a controlled CUI worksheet?

   Answer: Yes, if you are on an authorized system accredited at the appropriate level.

4. **Question:** Going back to the role of DCSA, can it file a CUI violation on industry during their security review?

   Answer: Industry follows the National Industrial Security Program Operating Manual (NISPOM), which doesn't cover CUI. I do understand the customer may require it. Yes, DCSA can report CUI violations identified during a security review. Paragraph 3.9.c of DODI 5200.48 states “The DOD Components’ CSAOs and CPMs will establish procedures to ensure prompt and appropriate management action is taken in cases of CUI misuse, including Unauthorized Disclosure (UD) of CUI, improper CUI designation and marking, violation of this issuance, and incidents potentially placing CUI at risk of UD.”

The NISPOM does cover some aspects of CUI and states that while outside the requirements of the NISPOM, when a classified contract includes provisions for CUI training, contractors will comply with those contractual requirements. It further states that contractors will comply with marking and safeguarding in accordance with contract requirements.

5. **Question:** There isn't solid guidance on what the correct categorizations of CUI the systems such as NISS and DISS/NBIS are. When is that information going to be disseminated?

   Answer: That determination will be made by the system owners.

6. **Question:** Can USD(I&S) send out a DOD-wide memo stating that the CUI warning statement is no longer required?

   Answer: No. The removal of the CUI warning statement is included in Change 1 of DODI 5200.48, which will be published later this year.

7. **Question:** Should DD Form 254 Contract Security Classification Specification include CUI markings?

   Answer: Generally, not, but it does depend on what information is included on the DD Form 254. Seek guidance from your agency/component.

8. **Question:** Can DOD SAFE be used by industry?

   Answer: Government personnel working with an industry partner can send them a link to submit to the government via DOD SAFE via the “Request a Drop-off" feature in the app.

9. **Question:** On Unclassified REL TO, would that change the banner lines or would it still remain "CUI”.

   Answer: DOD policy states that “CUI” will be the only marking in the banner line. All CUI category and dissemination information goes in the CUI Designation Indicator (DI) block.

10. **Question:** As cloud-based systems become more prevalent, will there be training provided on the FedRAMP requirements and CUI.

    Answer: The DOD CUI regulatory guidance, DODI 5200.48, section 3.3 Handling Requirements, provides guidance in reference to any systems/network that store, process, or transmit CUI, stating that they must "be categorized at the "moderate" confidentiality impact level and follow the guidance in DODIs 8500.01 and 8510.01. This applies to Federal Risk and Authorization Management Program (FedRAMP) and cloud-based systems.

    For contractual and Industry-related guidance, review Section 5 of DODI 5200.48 "Application to DOD Industry."

    Other related resources

    - DOD Procurement Toolbox
    - NIST SP 800-53