

MEMORANDUM FOR Combined Arms Center (CAC) Personnel

SUBJECT: Controlled Unclassified Information (CUI) Training

1. Reference: CAC Operations Order (OPORD) 16-362-003, SUBJECT: Data Call for AR 350-1 Individual Training Tasks for CAC Monthly Performance Analysis and Review (PAR) with the DtCG, 27 Dec 16.

2. Purpose: This memo provides an overview of the Army's CUI Program and satisfies the CUI training requirement outlined in reference 1.

3. Facts: DoD Manual 5200.01, Volume 4, DoD Information Security Program, Controlled Unclassified Information (CUI), 24 Feb 12 provides regulatory guidelines on all aspects of the CUI program. The Department of Defense and the US Army use the term "FOR OFFICIAL USE ONLY (FOUO) to mark their CUI.

4. Definition: FOUO is a dissemination control applied by DoD and the Army to unclassified information when disclosure to the public would reasonably be expected to cause a foreseeable harm to an interest protected by one of more of the Freedom of Information Act (FOIA) Exemptions 2 – 9. Information on FOIA exemptions is found in AR 25-55, The Department of the Army Freedom of Information Act Program, 1 Nov 77. Users will not apply the FOUO marking to documents unless the documents meet a FOIA exemption criteria.

5. Production: The originator of a document is responsible for determining whether or not the information in the document contains FOUO information and should be marked FOUO. This responsibility does not preclude competent authority (officials higher in chain of command/functional experts) from modifying the FOUO marking applied by the originator or adding FOUO markings. The higher authority must notify the document's originator if he/she makes changes. The document originator must portion mark all paragraphs of the FOUO document to ensure the reader understands what information is FOUO and what information is unclassified. The originator must also mark the bottom of the cover sheet, the title page, the first page, the outside of the back cover and all pages containing FOUO information with FOR OFFICIAL USE ONLY. Originators may contact their organization's security manager or refer to DoD Manual 5200.01, Volume 4 for more information on document marking.

6. Transmission: Users will encrypt all FOUO documents prior to e-mailing them and will not send FOUO documents to personal email addresses.

7. Sharing / Release. No person may have access to FOUO unless that person has a valid need for such access in connection with the accomplishment of a lawful and authorized US Government mission.

ATZL-CSI

SUBJECT: Controlled Unclassified Information Training (CUI)

a. Public: FOUO documents are not releasable to the public nor may they be posted on publicly accessible websites without review and release by the organization's Operations Security (OPSEC) Officer and Public Affairs Officer (PAO). Once these individuals approve the documents for release, the documents become public domain information and the FOUO markings are removed.

b. Contractors: FOUO documents are not releasable to contractors unless the documents support the contract and the contract states that the contractors may receive FOUO information.

c. International Personnel: FOUO documents are not releasable to international personnel without coordination through the organizational security manager to the CoE G2 Foreign Disclosure Officer (FDO).

8. Storage: Users will protect FOUO during and after work hours. Users will also place a DA Label 87 cover sheet on all printed FOUO documents and will store FOUO information in a locked desk, file cabinet or office when not in use.

9. Destruction: Users will shred all FOUO material in shredders approved for unclassified or classified destruction.

10. Unauthorized Disclosure: No formal security inquiry or investigation is required for unauthorized disclosures of FOUO information. Organizational leadership will take appropriate action to fix responsibility for the unauthorized disclosure to preclude it from happening again

11. Questions concerning FOUO information may be directed to the organizational security manager.

Local MSCoE questions regarding CUI can be referred to the Alt Command Security Manager at **573-563-5933**.

Organization

Signature

Date