DOD Unauthorized Disclosure Desk Reference

Important Definitions

Unauthorized Disclosure (UD)	Communication or physical transfer of classified or controlled unclassified information (CUI) to an unauthorized recipient
Compromise	A security incident in which there is a UD of classified information
Data Spill	Transfer of classified or CUI to a computer system accredited at a lower classification level than the data being entered

UD PMO

The **Unauthorized Disclosure Program Management Office (UD PMO)** was realigned from the Office of the Under Secretary of Defense for Intelligence to DSS on December 16, 2016. UD PMO was aligned within DSS to the **DOD Insider Threat Management and Analysis Center (DITMAC)**. The realigned UD Program provides enterprise level management and operational capability to improve the identification, investigation, tracking, and reporting of UDs.

Contact Information

Phone: 571-357-6875
NSTS: 982-3613
Email:
NIPR: dcsa.quantico.hq.mbx.ditmac-unauthorized-disclosure@mail.mil
SIPR: dcsa.quantico.hq.mbx.ditmac-unauthorized-disclosure@mail.smil.mil
JWICS: DITMAC.UD@dss.ic.gov

Required Documentation

Preliminary Inquiry

- **What is it?** Initial fact finding and analysis process to determine the facts of any security incident
- **When is it required?** All cases where information is compromised
- **What is included?** Who, what, when, where, how
- **When should it be completed?** As soon as possible, not to exceed 10 duty days

Damage Assessment

- **What is it?** Formal multidisciplinary analysis to determine the effect of a compromise of classified information on national security
- **When is it required?** All cases where information is compromised
- **What is included?** Practical effects of a compromise on DOD programs, operations, systems, materials, and intelligence and on the Department of Defense's ability to conduct missions
- **When should it be completed?** Within six months

Media Leaks Questionnaire

- **What is it?** Questionnaire required to refer a UD in the media to the Department of Justice (DOJ)
- **When is it required?** If the disclosure was in the public domain
- **What is included?** 11 specific questions
- **When should it be completed?** As soon as practical

UDs Reportable to UD PMO

All UDs are serious, but not all need to be reported to UD PMO. The following will be reported to UD PMO (even when attribution has not been made):

Media	The release of classified information and/or controlled unclassified information in the public domain. Public domain includes and is not limited to podcast, print articles, internet-based articles, books, journals, speeches, television broadcasts, blogs, and postings.
Technology	Release and/or enabled theft of information relating to any defense operation, system, or technology determined to be classified and/or controlled unclassified information.
Unauthorized Recipient	Information wherein individual disclosed classified information and/or controlled unclassified information to unauthorized person or persons resulting in administrative action, referral for criminal and/or CI investigation, and/or resulted in the suspension or revocation of eligibility.

Reporting Media Leaks to the Department of Justice

When UD PMO receives a confirmed report of a UD in the media, we are required to submit a UD referral to the DOJ. In addition to the preliminary inquiry and damage assessment required by all security violations, all UD in the media require the completion of a media leaks questionnaire. This reporting process to DOJ utilizes a tiered approach based on the action DOD would like DOJ to take.

Tier I	The Component's inquiry or investigation determines that further investigation is not warranted. DOD does not ask for further action from DOJ
Tier II	DOD has determined that an internal or administrative investigation is appropriate
Tier III	DOD is requesting a criminal investigation from DOJ

* current 6/21/2023

DOD Controlled Unclassified Information Reference

What is CUI

Controlled Unclassified Information (CUI)	Unclassified 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.

The CUI Program was created with the issuance of the DODI 5200.48 on March 6, 2020 & the cancellation of DODM 5200.01, Vol. 4 with its legacy markings of "For Official Use Only (FOUO), Law Enforcement Sensitive (LES), etc.

Controlled unclassified information requiring protection at all times in a manner minimizing the risk of unauthorized disclosure while allowing for access by entities with an authorized, lawful government purpose.

CUI Registry

Provides information, guidance, training, and requirements for handling CUI at the national level. The official CUI Registry is found on the Information Security Oversight Office (ISOO) website: https://www.archives.gov/cui. For the DOD CUI Registry visit https://www.dodcui.mil.

CUI Training

The DODI 5200.48 requires successful completion of the DOD Mandatory CUI Training module found on the CDSE website: https://securityawareness.usalearning.gov/cui/index.html or the DOD CUI website: https://www.dodcui.mil for everyone with access to CUI. This training addresses the eleven required elements. It provides an overview of the various components of the CUI Program.

Sharing & Safeguarding CUI

When to share CUI: If access promotes a common project or operation between agencies or under a contract or agreement.
When NOT to share CUI: If access harms or inhibits a common project or operation between agencies or under a contract or agreement.

Physical	CUI must be stored or handled in controlled environments that prevent or detect unauthorized access such as locked drawers or file cabinets. CUI must have at least one layer of protection during transport. CUI cannot be discussed on wireless devices nor printed on home computers.
Technology	IT systems must protect from unauthorized access & be set at moderate confidentiality level; Send CUI only from a ".mil or .gov" account or government authorized industry email; Emails must be encrypted; DoD SAFE may be used for CUI.
Contracts	The **government must** identify CUI in both unclassified & classified contracts to ensure safeguards & controls are employed while the CUI is being used by the contractors. Non-DOD systems must be in compliance with NIST SP 800-171 requirements to process, store, & transmit CUI.

Limited Dissemination Controls

LDCs are to be placed on unclassified documents and other materials when the CUI requires access restrictions, including those required by law, regulation, or government-wide policy.

Control	Marking
No Foreign Dissemination	NOFORN
Federal Employees Only	FED ONLY
Federal Employees and Contractors Only	FEDCON
No Dissemination to Contractors	NOCON
Dissemination List Controlled	DL ONLY
Authorized for Release to Certain Foreign Nationals Only	REL TO USA
Display Only	DISPLAY ONLY
Attorney Client	ATTORNEY-CLIENT
Attorney Work Product	ATTORNEY-WP

Distribution Statements

Distribution Statements (B-F), based on DODI 5230.24, are to be placed on CUI documents & other materials when: the CUI category is Controlled Technical Information (CTI); contains Scientific, Technical, and Engineering Information; and Export Controlled Technical Information.

UDPMO

The **Unauthorized Disclosure Program Management Office (UD PMO)** was realigned from the Office of the Under Secretary of Defense for Intelligence & Security to the former DSS, now DCSA, on December 16, 2016. The UD PMO aligns within DCSA to the **DOD Insider Threat Management and Analysis Center (DITMAC)**. Incidents involving the unauthorized release of CUI in the public domain must be reported to the Security Manager & the UD PMO immediately.

Contact Information

Phone: 571-357-6875
NSTS: 982-3613
Email:
dcsa.quantico.hq.mbx.ditmac-unauthorized-disclosure@mail.mil
dcsa.quantico.hq.mbx.ditmac-unauthorized-disclosure@mail.smil.mil
DITMAC.UD@dss.ic.gov

* current 6/21/2023