2023

How to Respond to an Unauthorized Disclosure (UD) of Classified and Controlled Unclassified Information (CUI)

Center for Development of Security Excellence

CDSE *training*

Disclaimer: All the information in this document is derived from references but not verbatim from policy. Please also refer to your component specific guidance. For incidents occurring at contractor locations, please follow guidance in the 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM) and the DCSA Security Incident Job Aid.

Reference: DODM 5200.01 Vol. 3: Protection of Classified Information

	Person(s) Responsible **Individual Who Discovered the Unauthorized Disclosure (UD)**
Steps	**Action**
Safeguard	Take custody of and safeguard the material if possible and immediately notify the appropriate security authorities (i.e., keep the material in your direct possession until it can be secured in a General Services Administration (GSA) approved security container, or you can surrender control of the material to the owner or your local security official). (***Note:*** *If classified information appears in the public media, including on public internet sites, or if a representative of the media approaches you, please refer to DODM 5200.01 Vol. 3; do not respond to the information if it is on social media, and do not print it if it is from a digital media outlet.)*
Report	All personnel should report the incident to the DOD Activity Security Manager. • If the Activity Security Manager is believed to be involved, report to security authorities at the next higher level. • When contractors are involved in an incident at a DOD component, they must also report to their company and Facility Security Officer (FSO).

	DOD Activity Security Manager
Steps	**Action**

Inquire	Conduct an inquiry to determine who, what, when, where, why, and how:
	
	• Who is responsible for the UD?
	• What actions led to the UD?
	  ○ What person, situation, or conditions caused or contributed to the incident?
	  ○ Was there a compromise of classified information?
	  ○ If a compromise occurred, what specific classified information and/or material was involved?
	  ○ What is the classification level of the information disclosed?
	  ○ What corrective action is required?
	• When did the UD occur?
	• Where did the UD occur?
	• Why did the UD occur?
	• How did the UD occur?

Investigate	Conduct an investigation for a security violation when the incident cannot be resolved via inquiry or for incidents where an in-depth and comprehensive examination of the matter is appropriate: • For DOD incidents, initiate and conduct the investigation at the lowest level possible within the component.
Evaluate	Review the results of the inquiry/investigation and determine if an infraction or a violation occurred: • An infraction occurs when there is a failure to comply with requirements but no classified information is lost or compromised. • A violation occurs when classified information is lost or compromised or could be expected to result in loss or compromise.
Elevate	Elevate the results of the investigation as follows: • Always report to the Original Classification Authority (OCA) who will conduct a damage assessment. • Report to information owners for special categories. This depends on the category of the compromised information. Example: A UD of design specification for a classified nuclear aircraft carrier component firing control may fall under a Restricted Data (RD) Program such as Critical Nuclear Weapon Design Information (CNWDI). • DOD UD Reporting: Depends on the category of information that has been compromised: o Notify the Unauthorized Disclosure Program Management Office (UD PMO) of all UDs involving classified information in the public domain. o Notify the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) of UDs that involve espionage, UDs in the public media or domain, or any UD incident where Congressional reporting may be required, including Sensitive Compartmented Information (SCI) or Special Access Programs (SAPs). o Spillage: Notify the Information System Security Manager (ISSM) in addition to the OCA. o OUSD (I&S) must report to Congress, on behalf of the Secretary of Defense (SecDef), each security or counterintelligence failure or compromise of classified information that the Secretary determines is likely to cause significant harm or damage to national security.
Correct	Take remedial actions to prevent recurrence based on the results of the investigation. These actions should focus on correcting or eliminating the conditions contributing to the incident.

Reference: DODI 5200.48: Controlled Unclassified Information (CUI)

For UD of CUI, no formal security inquiry or investigation is required unless disciplinary action against the individual(s) responsible is taken. In such cases, an inquiry is appropriate. UD of certain CUI, such as export controlled–technical data, may also result in potential civil litigation and criminal penalties against responsible persons based on the procedures codified in the relevant law, regulation, or government-wide policy. The DOD Component originating the CUI will be informed of any UD.

Report misuse or mishandling of UD of CUI to the UD Program Management Office (UD PMO).

(***Note:*** *It is recommended only substantiated cases that need to be referred to the Department of Justice (DOJ) or Military Department Counterintelligence Organizations (MDCOs) for possible criminal prosecution or Uniform Code of Military Justice (UCMJ) charges be referred to UD PMO; the Component's security office or equivalent entity should track and maintain the metrics.)*

	Person(s) Responsible **Individual Who Discovered the UD of CUI**
Steps	**Action**
Safeguard	Immediately take possession of the material and safeguard it if possible or secure it in a controlled environment. The concept of a controlled environment means there is sufficient internal security measures in place to prevent or detect unauthorized access to CUI until you can surrender control of the material to the owner or your local security official. (***Note:*** *Do not respond to the information if it is on social media, and do not print it if it is from a digital media outlet.)*
Report	All personnel should report the incident to their security office or equivalent entity.
	DOD Activity Security Manager
Steps	**Action**

Inquire	Determine if an inquiry/investigation is necessary.
	
	Conduct an inquiry to determine the who, what, when, where, why, and how:
	
	• Who is responsible for the UD?
	• What actions led to the UD?
	  ○ What person, situation, or conditions caused or contributed to the incident?
	  ○ Was there a compromise of CUI?
	  ○ If a compromise occurred, what specific category of CUI and/or material was involved?
	  ○ What corrective action is required?
	• When did the UD occur?
	• Where did the UD occur?
	• Why did the UD occur?

	• How did it occur?
Investigate	Conduct a formal inquiry/investigation in coordination with the appropriate officials: • For DOD incidents, the Component initiates the investigation.
Evaluate	Review the results of the inquiry/investigation and determine notifications: • Does the UD warrant that disciplinary action be taken against the individual(s)?
Elevate	Elevate the results of the investigation as follows: • Notify the UD PMO. In addition, notify the appropriate MDCO of all incidents.
Correct	Take remedial actions based on the results of the investigation. These actions should focus on correcting or eliminating the conditions contributing to the incident.

Resources to Support UD Reporting

Defense Office of Prepublication and Security Review (DOPSR)

Department of Justice (DOJ)

DOD Hotline Information

Military Department Counterintelligence Organization (MDCO) (access the various MDCOs through the military department website)

Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S))

Unauthorized Disclosure Program Management Office (UD PMO)