Unauthorized Disclosure of Classified Information and Controlled Unclassified Information

Student Guide

January 2025

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Welcome

Course Overview

Unauthorized disclosures of classified national security information (CNSI) and controlled Unclassified information (CUI) make headlines—and for good reason. This information, in the wrong hands, can cause catastrophic outcomes for our national and operational security, as well as Department of Defense (DOD) employees, military personnel, contractors, and resources. This course will examine ways that you can protect this sensitive information and present examples of unauthorized disclosure including headlines such as Daniel Hale, who leaked information on U.S. drone warfare and was sentenced to 45 months in prison; the OPM data breach, in which the records of millions of government personnel and contractors were hacked; Henry Frese, a former DIA employee who pled guilty to leaking classified national defense information to journalists; and Bryan Martin, a Sailor charged with espionage and attempting to sell classified information.

Course Objectives

Welcome to the *Unauthorized Disclosure of Classified Information and Controlled Unclassified Information* course. Take a moment to review the course objectives:

- Given a scenario, assess whether an action is an unauthorized disclosure of Classified National Security Information (CNSI) or Controlled Unclassified Information (CUI).
- Given a scenario, apply Department of Defense (DOD) policy requirements to protect CNSI and CUI from unauthorized disclosure.
- Given a scenario, determine the required steps for reporting an unauthorized disclosure.

Lesson 2: Unauthorized Disclosure Overview

Introduction

Lesson Overview

Welcome to the *Unauthorized Disclosure Overview* lesson.

Public service is a public trust. All personnel must prevent unauthorized disclosure (UD) of non-public Department of Defense (DOD) information for any reason. UD of classified national security information (CNSI) or controlled Unclassified information (CUI) to the public or unauthorized recipients, has many negative effects. It reduces the effectiveness of DOD management, damages intelligence and operational capabilities, and lessens the DOD's ability to protect critical information, technologies, programs, Service members, and personnel.

As directed by the Secretary of Defense in a memo dated April 17, 2023, "Adverse security incidents are a stark reminder that adherence to required security procedures underpin all aspects of the DOD mission, and we must continually reinforce these requirements to keep pace with evolving threats." In addition, "Leaders must reinforce their expectation that their workforce will immediately report all security incidents to the chain of command and their security manager or the Office of their Inspector General and must ensure that individuals in their workforce are empowered to make these reports."

Lesson Objectives

Take a moment to review the lesson objectives.

- Given a scenario, assess whether an action is an unauthorized disclosure (UD) of Classified National Security Information (CNSI) or Controlled Unclassified Information (CUI).
  - Given an example of a UD, determine its type.
  - Given examples, determine misconceptions about UD.
  - Given an example, determine whether it is a UD or a protected disclosure under the Whistleblower Protection Enhancement Act (WPEA).
- Given a scenario, apply DOD policy requirements to protect CNSI and CUI from unauthorized disclosure.
  - Given an example, characterize the damage caused by a UD.

Definitions and Policies

Initial Definitions

UD is the communication or physical transfer of CNSI or CUI to an unauthorized recipient. An unauthorized recipient is anyone who does not meet the criteria to access the information, whether that is access requirements for CNSI or the required lawful, government purpose to access CUI.

Often, UD is committed by an insider. An insider is someone who has or had been granted eligibility for access to CNSI or eligibility to hold a sensitive position. UD can also be committed by a remote actor, which is an individual outside of the organization who has gained unauthorized access to CNSI or CUI. Insiders with trusted access, as well as remote actors, may pose harm to national security through espionage, terrorism, or unauthorized disclosure of national security information.

CNSI

For authorized access to CNSI, an individual must have:

- A signed Standard Form (SF) 312, Classified Information Non-Disclosure Agreement (NDA)
- Eligibility at the appropriate level
- A confirmed need-to-know

CUI

For authorized access to CUI, an individual must have a lawful, government purpose to access the information. Authorized holders of CUI are responsible for determining who has a lawful, government purpose. Unlike classified information, an individual or organization generally does not need to demonstrate a need-to-know to access CUI, unless it is required by a specific law, regulation, or government-wide policy. Although need-to-know does not typically apply, CUI should only be shared when it will help achieve the goals of a common mission or project.

Intent and Impact of UD

The potential harm that may come from UD is caused by various levels of intent. These include willful, negligent, and inadvertent UD.

An incident is considered willful if the person purposefully disregards DOD security or information safeguarding policies or requirements. An example of willful UD is an

individual intentionally bypassing a known security control, such as an individual with access intentionally disclosing classified information in the public domain.

An incident is negligent if the person acted unreasonably, causing UD. An example of negligent UD is a careless act or reckless disregard for proper procedures such as an individual who carelessly shares classified information via an Unclassified network leading to spillage.

An incident is inadvertent if the person did not know, and had no reasonable basis to know, that the security violation or unauthorized disclosure was occurring. An example of inadvertent UD would be an individual who reasonably relied on security classification markings in an authorized source document that was later determined to be improperly marked.

Regardless of the intent of UD, when it occurs, UD results in the loss or degradation of resources or capabilities, undermines DOD's mission and security, damages public trust, and compromises sources and methods.

Key Policies

To safeguard against UD, there are several key policies governing CNSI and CUI requirements. These include Executive Orders (E.O.s); Federal regulations; and DOD regulatory guidance, including Manuals, Directives, Instructions, and Memos.

Executive Orders

E.O.s that apply to CNSI or CUI are:

- E.O. 13526, Classified National Security Information
- E.O. 13556, Controlled Unclassified Information

Federal Regulations

Federal regulations that apply to CNSI or CUI include:

- 32 Code of Federal Regulations (CFR) Part 117, National Industrial Security Program Operating Manual (NISPOM)
- 32 CFR Part 2002, Controlled Unclassified Information
- 32 CFR Part 2001 and 2003, Classified National Security Information
- 32 CFR Part 2004, National Industrial Security Program

DOD Guidance

The following DOD issuances apply to CNSI or CUI:

- DOD Manual (DODM) 5200.01, Volume 1, DOD Information Security Program: Overview, Classification, and Declassification
- DODM 5200.01, Volume 2, DOD Information Security Program: Marking of Information
- DODM 5200.01, Volume 3, DOD Information Security Program: Protection of Classified Information
- DOD Directive (DODD) 5210.50, Management of Serious Security Incidents Involving Classified Information
- DOD Instruction (DODI) 5230.09, Clearance of DOD Information for Public Release
- DODI 5230.29, Security Policy and Review of DOD Information for Public Release
- DODI 5200.48, Controlled Unclassified Information
- DODI 8500.01, Cybersecurity
- DODI 8510.01, Risk Management Framework for DOD Systems
- Memo: Security Review Follow-on Actions – June 30, 2023
- Memo: Immediate Review and Assessment of DOD Information Security Procedures – April 17, 2023

In addition, the Intelligence Community (IC) issued Intelligence Community Directive (ICD) 701, Unauthorized Disclosure of Classified National Security Information.

UD Types

UD policies were put in place to protect against various types of UD. Do you know the difference between each type of UD?

Consider this scenario. Lily has access to Top Secret information. She is selected to do an interview about her role within the DOD and during the interview, she discloses Top Secret program information. The journalist who interviewed her publishes the information. Do you think you know the type of UD that has occurred here?

Think about this scenario as you learn about the various types of UD.

UD Type Definitions

As we just mentioned, there are several types of UD. These include public domain, spillage, espionage, and improper safeguarding of information. There are also additional special circumstances concerning unauthorized disclosures.

Public Domain

A UD in the public domain occurs when CNSI or CUI is released either intentionally or inadvertently to the public. There are several different mediums that comprise UD in the public domain, including:

- Podcasts
- Print or web-based articles
- Books
- Journals
- Speeches
- Television broadcasts
- Blog postings
- Social media posts on a group or private social media page
- Instant messages shared on a social media platform
- Voice Over Internet Protocol (VOIP) social platforms, such as Discord, Zoom, or Skype
- Protected or encrypted messaging apps, such as WhatsApp or Signal

Spillage

A data spill, or spillage, is a willful, negligent, or inadvertent disclosure of CNSI or CUI transferred onto an information system not accredited at the appropriate security level to store, process, or transmit the information.

Classified spillage occurs when classified data is introduced either onto an Unclassified information system, an information system with a lower level of classification, or to a system not accredited to process data of that restrictive category.

CUI spillage occurs when it is stored, processed, or transmitted by a DOD information system not in compliance with DODI 8500.01, “Cybersecurity” and DODI 8510.01, “Risk Management Framework for DOD Systems.” For non-DOD information systems, CUI spillage occurs when not in compliance with DODI

8582.01, “Security of Non-DOD Information Systems Processing Unclassified Nonpublic DOD Information.”

Espionage

Espionage involves activities designed to obtain, deliver, communicate, or transmit CNSI or CUI intended to aid a foreign power.

Improper Safeguarding

Improper safeguarding of information occurs when inappropriate measures, behaviors, or controls are used to protect CNSI or CUI.

Special Circumstances

There are special circumstances concerning UDs that require unique handling or the consideration of additional reporting requirements.

For UD incidents related to Foreign Government Information (FGI) or North Atlantic Treaty Organization (NATO) information, further reporting is required. Any UDs involving criminal activity require coordination with the Deputy Chief Information Officer (DCIO) during the investigation. Finally, UDs involving special information, such as Sensitive Compartmented Information (SCI), Special Access Program (SAP) information, and Critical Program Information (CPI) have additional reporting requirements.

UD Type Activity

Example 1 of 4. Lily has access to Top Secret information. She is selected to do an interview about her role within the DOD and during the interview, she discloses Top Secret program information. The journalist who interviewed her publishes the information. What type of UD is this?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Spillage
- ○ Public domain
- ○ Espionage
- ○ Improper safeguarding

Example 2 of 4. Ted is working with a potential DOD contractor for a new project. The contractor asks Ted for CUI related to the contract, and Ted sends the CUI from his DOD Information System via unencrypted email. What type of UD is this?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Spillage
- ○ Public domain
- ○ Espionage
- ○ Improper safeguarding

Example 3 of 4. Erin works as a defense intelligence analyst studying a near peer country's drone production. She works closely with allied foreign partner analysts, but always on separate problem sets. One of the allied analysts in particular, Jerome, concentrates on the near peer's government equities, but has lately been asking Erin a lot of questions regarding the country’s drone capabilities - which is outside his problem set. Jerome does not have a need-to-know but is very persistent. What type of UD is this?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Spillage
- ○ Public domain
- ○ Espionage
- ○ Improper safeguarding

Example 4 of 4. While working with paper copies of Secret information, Marshall leaves the secure area to use the restroom. He leaves the Secret documents on the restroom counter, and they are later discovered by an uncleared facility custodian. What type of UD is this?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Spillage
- ○ Public domain
- ○ Espionage
- ○ Improper safeguarding

Misconceptions

Misconceptions

Can you distinguish fact from fiction when it comes to UD? For example, once CNSI or CUI is in the public domain, can you discuss it openly? Does your SF 312 NDA still apply after you leave your organization? Misconceptions like these can easily result in UDs.

Realities

As you've just learned, common misconceptions can all too easily result in UDs. So, what is the reality?

Public Domain

Even if CNSI or CUI appears in the public domain, such as in an online news article or on a social media posting, the information is still protected. That means CNSI is still classified until an official declassification decision has been made and the information has gone through the prepublication review process. In the case of CUI, it is still designated as CUI until it has been decontrolled and gone through the prepublication review process.

Journalist Privilege

Employees cannot be afforded protection under journalist privilege if they disclose CNSI or CUI to a reporter or journalist. Journalist privilege allows reporters and journalists to protect their sources during grand jury proceedings.

Publishing

A security review from the Defense Office of Prepublication and Security Review (DOPSR) ensures classification by compilation does not occur. Classification by compilation occurs when Unclassified information is combined and something new is revealed that qualifies as classified, by putting all of the pieces together that is not revealed by the Unclassified individual parts. A DOPSR review is required for classified and declassified CNSI, controlled and decontrolled CUI, and Unclassified information.

SF 312

The SF 312 NDA you sign is a lifetime agreement with the federal government. To learn more, visit the Termination Briefing Short offered by CDSE.

Messaging Apps

DOD information that has not been cleared for public release should not be shared on any messaging apps not controlled by the DOD, no matter how secure you perceive it to be. These apps may be subject to search, data mining, and other data correlation tools that may lead to spillage via classification through compilation. Classification by compilation occurs when Unclassified information is combined and something new is revealed that qualifies as classified, by putting all of the pieces together that is not revealed by the Unclassified individual parts.

Misconceptions Activity

Check your understanding of UD misconceptions. Which of these is a misconception related to UD?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ It is okay to read, discuss, and freely share CNSI or CUI that has been put in the public domain.
- ☐ You may receive protection through “journalist privilege” if you disclose CNSI or CUI to a journalist.
- ☐ Manuscripts, books, etc., can be submitted to an editor or publisher before undergoing a security review.
- ☐ Once I leave my organization, the SF 312 NDA no longer applies.
- ☐ It is okay to share Unclassified DOD information on a “secure” messaging app.

Whistleblowing

Whistleblowing

Can you tell the difference between whistleblowing and UD? You may think you are doing the right thing when it comes to disclosing information you have access to, but there are guidelines for reporting when you believe national security is at risk.

With that in mind, let’s consider a scenario. An insider believes the government poses a danger to the public and releases national security information on a social networking site to make the public aware of the danger. Is this whistleblowing or unauthorized disclosure?

We’ll review the guidelines for whistleblowing, then you will have the opportunity to answer this question.

Whistleblowing Definitions

In the scenario we reviewed, an individual leaked information, believing they needed to make the public aware of a national security issue. To help you figure out whether or not that is whistleblowing, let's review an example that constitutes whistleblowing.

John, an intelligence analyst with the DOD, is directed by his boss, Bill, to falsify intelligence information. John reports Bill's directive to the DOD Inspector General, who initiates an investigation into the matter.

To qualify as "whistleblowing," an individual must provide the right information to the right people while still protecting national security assets from unauthorized disclosure by following the required procedures. It occurs when employees report information they reasonably believe provides evidence of:

- A violation of any law, rule, or regulation
- Gross mismanagement
- A gross waste of funds
- Abuse of authority
- A substantial danger to public health and safety

Whistleblower Protection Statutes

To protect whistleblowers, the government has enacted statutes, including the Whistleblower Protection Enhancement Act (WPEA) of 2012. This broadened the scope and strengthened the rights and protections of federal employees who blow the whistle on violations involving fraud, waste, and abuse. When reporting violations involving classified programs or information, employees must be mindful that established guidance for protecting classified information still applies.

Whistleblower guidance is outlined in:

- Presidential Policy Directive (PPD) 19, which protects employees in the intelligence community or employees having access to classified information
- Title 5, United States Code, or U.S.C, Section 2302 – "Prohibited Personnel Practices", which provides for appropriated fund civilian reprisal
- Title 10, U.S.C., Section 1034 "Military Whistleblower Protection Statute", which provides for military reprisal and restriction
- Title 10, U.S.C., Section 2890, "Right and responsibilities of tenants of Housing Units", which provides for privatized military housing

- Title 10, U.S.C., Section 1587 “Non-appropriated Fund Instrumentality: Employees Whistleblower Protections”
- Title 10, U.S.C., Section 4701 “Contractor Employees: Protection from Reprisal for Disclosure of Certain Information”, which provides defense contractor, subcontractor, grantee, and subgrantee, and personal services contractor reprisal

To learn more, visit the DOD Inspector General website through the course resource page.

Whistleblowing Activity

Let’s revisit the scenario we introduced earlier. Can you determine whether or not it is whistleblowing? Remember, in this scenario an insider believes the government poses a danger to the public and releases national security information on a social networking site to make the public aware of the danger. Is this whistleblowing or unauthorized disclosure?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Whistleblowing
- ○ Unauthorized Disclosure

Damage

Damage

Now that you’ve learned about UD and protections for whistleblowers, let’s review what could happen as a result of unauthorized disclosure.

While you are scrolling social media, you happen to see a post from one of your coworkers. This coworker has disclosed CUI on their private social media account. Can this disclosure result in damage? Keep your answer in mind. You’ll get a chance to answer it after we review the possible damages caused by UD.

Consequences of Unauthorized Disclosure of CUI

The UD of CUI can have serious consequences such as a direct impact on national security through leaks, espionage, and spillage. Other impacts include adverse effects on an organization’s operations, assets, and personnel. The UD of CUI can significantly reduce or negatively impact mission capabilities and the effectiveness of

primary functions. It can also cause significant financial loss to an organization and damage an organization's assets.

Consequences of Unauthorized Disclosure of CNSI

When information meets the criteria for classification under Section 1.4 of E.O. 13526, its classification is based on the level of describable damage that the unauthorized disclosure of that information could reasonably be expected to cause to national security. These categories are:

- Top Secret, which can lead to exceptionally grave damage to national security
- Secret, which can cause serious damage to national security
- Confidential, which can cause damage to national security

Unauthorized disclosure of CNSI can lead to the loss of sensitive information to bad actors which can place warfighters in harm's way. It can also waste national resources, which include time, money, and effort, as well as reduce the effectiveness of the DOD.

Damage Activity

Let's revisit the scenario we introduced you to earlier. Do you know the correct response?

While you are scrolling social media, you happen to see a post from one of your coworkers. This coworker has disclosed CUI on their private social media account: "Check out this upcoming draft DOD policy I was asked to review this week – can you believe these changes?" Can this disclosure result in damage?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Flag post – this can cause damage
- ○ No issue – the information isn't classified

Case Study: Daniel Hale

As we've discussed, the unauthorized disclosure of CUI and CNSI can cause significant damage to national security. Let's review a case where this occurred in real life: Daniel Hale.

Daniel Hale was a former enlisted airman, an analyst at the National Security Agency (NSA), and a defense contractor to the National Geospatial-Intelligence Agency (NGA). He held Top Secret/Sensitive Compartmented Information (TS/SCI)

eligibility and was entrusted with access to classified national defense information. Between December 2013 and August 2014, while working at NGA, Hale took classified documents for the purpose of anonymously “leaking” information to a reporter because he was anti-war and opposed the use of drone warfare. These classified documents were published and available for anyone to view, potentially causing exceptionally grave damage to the U.S.

Conclusion

Lesson Summary

You have completed the *Unauthorized Disclosure Overview* lesson.

Lesson 3: Life Cycle Protection Requirements

Introduction

Lesson Overview

Welcome to the Life Cycle Protection Requirements lesson.

Classified national security information (CNSI) and controlled Unclassified information (CUI) must be protected throughout the life cycle of each. Protecting CNSI and CUI from unauthorized disclosure (UD) is supported throughout the information's life cycle by adhering to requirements for access, marking, and sharing. It is also protected by safeguarding when handling and properly storing the information. Finally, CNSI and CUI are protected from UD by adhering to requirements for declassifying classified information or decontrolling CUI and destroying and disposing of materials.

In this lesson, you will learn about the protection requirements for CNSI and CUI throughout their life cycles. Take a moment to review the lesson objectives.

- Given a scenario, apply DOD policy requirements to protect CNSI and CUI from unauthorized disclosure.
  - Given an example, identify access, safeguarding, marking, storage, dissemination, classification, declassification, and destruction requirements for CNSI.
  - Given an example, identify access, safeguarding, marking, storage, dissemination, decontrolling, and destruction requirements for CUI.

CNSI Requirements

Access to CNSI

Failure to ensure someone has met access requirements before sharing CNSI can lead to unauthorized disclosure (UD).

Do you know if someone has the authority to access CNSI? Consider how you prevent UD as you review this scenario. Don't worry – you don't have to answer this question yet. Keep the scenario in mind as you learn access requirements.

You have control of Secret CNSI for a project you are managing. You receive a request from Andrew, who holds eligibility at the appropriate security level and has

signed a Standard Form (SF) 312 for the CNSI you have in your control. Can you share this Secret CNSI with Andrew? Let's check your understanding of the requirements.

CNSI Access Requirements

Let's examine the requirements for CNSI access. The requirements for authorized access to CNSI include a favorable determination of eligibility at the appropriate security level, a "need-to-know," and a signed SF 312, Classified Information Nondisclosure Agreement (NDA).

The individual with authorized possession, knowledge, or control of the information has the final responsibility to determine whether the prospective recipient's official duties require them to possess or have access to CNSI. Additionally, the prospective recipient must have been granted the appropriate security clearance by the proper authority. Any individual who fails to meet these requirements is not authorized to access CNSI.

Access Activity

Now that you've learned the requirements to access CNSI, let's revisit the scenario from earlier.

You have control of Secret CNSI for a project you are managing. You receive a request from Andrew, who holds eligibility at the appropriate security level and has signed an SF 312 for the CNSI you control. Should you give Andrew access to the CNSI?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Yes, since he has signed an SF 312 and possesses eligibility, he is eligible to access classified information.
- ○ No, he must also have a "need-to-know" to access classified information.
- ○ No, he must have Top Secret eligibility in order to access classified information.
- ○ No, he must have a signed order from his superior in order to access classified information.

Safeguarding CNSI Intro

If you have been granted access to CNSI, one of the most important things to do to protect against UD is ensure that you are safeguarding it appropriately. Do you know

what measures to take to safeguard information in your possession? Let's analyze a scenario where safe handling is key.

You are working with paper copies of Top Secret information to prepare for an upcoming brief. While you walk from your desk to the briefing room, you want to ensure that no one can view the information who does not have access to it. In this situation, how would you protect it? Consider your response; you'll get a chance to test your understanding later in this lesson.

Safeguarding CNSI

To prevent UD, you need to know how to properly handle, transmit, and store CNSI. You will find guidance for protecting CNSI from unauthorized disclosure in:

- Executive Order (E.O.) 13526, Classified National Security Information
- DOD Manual (DODM) 5200.01, Volume 3, DOD Information Security Program: Protection of Classified Information
- Title 32 of the Code of Federal Regulations (CFR) Part 117, National Industrial Security Program Operating Manual (NISPOM)

Visit the course resources to access these, as well as relevant job aids.

When working with CNSI, you must ensure you safeguard it from unauthorized disclosure. You must properly handle CNSI. When you are ready to store CNSI, use GSA-approved containers, vaults, or approved open storage areas that meet classification level requirements.

When you need to reproduce CNSI, always follow reproduction guidelines. When sharing CNSI, follow appropriate procedures, including requirements for transmission and transportation of CNSI, and protecting CNSI at classified conferences and meetings.

Finally, when you are finished using CNSI, destroy and dispose of it in accordance with guidelines.

Please note, you are required to protect CNSI throughout your life, even when you are no longer affiliated with the federal government and/or military.

Safeguarding CNSI Activity 1

It's time to check your understanding. Let's revisit the scenario from earlier.

You are working with paper copies of Top Secret information to prepare for an upcoming brief. While you walk from your desk to the briefing room, you want to

ensure that no one can view the information who does not have access to it. In this situation, how would you protect it?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Protect it in a manila folder
- ○ Use an SF 703 cover sheet
- ○ Print a watermark identifying it as CNSI
- ○ Mark “Working Paper” on the first page

Safeguarding CNSI Activity 2

Next, you receive a request from a co-worker, Bianca, who is authorized to access the Secret information that you possess for a project she is working on. She is located in an office across the country from you. In this situation, how would you safely transmit the CNSI to Bianca?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Send it encrypted via an Unclassified email and request a read receipt
- ○ Send it on a properly accredited system via secure email after ensuring that Bianca has an accredited Secret level system
- ○ Send it via any commercial shipping service after ensuring Bianca can store it properly
- ○ Call Bianca on your work cell phone to share the critical information

Safeguarding CNSI Activity 3

You have been handling Secret information for a classified project you are working on all day and are ready to head home. In this situation, how would you safely store the CNSI before heading home, given that your work location does not have an approved open storage area?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Place it in a locked desk drawer
- ○ Place it in a GSA-approved container
- ○ Place it in a properly marked folder on your desk
- ○ Give it to your supervisor for safekeeping

Improperly Marked CNSI

Even if you are following proper safeguarding procedures, UD can occur unintentionally if a document is improperly marked. Let's look at a scenario where UD occurred because documents were improperly marked.

Sandra shared a document with a colleague. Later, after reviewing the document more carefully, she realized that it contains portion markings indicating Top Secret information – and her colleague does not hold Top Secret eligibility. She immediately reported the unauthorized disclosure to her supervisor. What could have prevented this UD?

Marking CNSI

As you saw in the previous example, CNSI that is not properly marked can lead to unintentional UD.

All CNSI must be clearly identified by authorized security classification markings, control markings and dissemination controls when applicable, and authorized portion markings. These markings must be conspicuous and immediately apparent. The purpose of these markings is to alert the holder that CNSI is present, identify the exact information needing protection, and the level of protection required.

Classification markings also give information on the sources of and reason for classification. For a derivatively classified document, this block will list "Derived from" rather than the reason. It should identify the office of origin and document originator, as well as guidance on downgrading and declassification of CNSI.

Finally, classification markings provide guidance on information sharing, and warn holders of special access, dissemination control, and safeguarding requirements when applicable.

To learn more about marking CNSI, access DODM 5200.01, Volume 2, through the course resources.

Marking CNSI Activity

Remember the scenario we discussed earlier? Now's the time to see what you've learned.

MEMORANDUM FOR XXXXXXXXXXXXXXX

SUBJECT: (U) Delegation of TOP SECRET Original Classification Authority (OCA)

(TS) You are hereby delegated authority to classify information up to TOP SECRET for information under your area of responsibility in accordance with Executive Order 13526, "Classified National Security Information" (the Order).

(C) As an OCA, you are required to receive training in original classification as provided by the Order and implementing directives prior to exercising this authority.

Sandra shared this document, which contains Top Secret information, with a colleague who does not hold Top Secret eligibility. What could have prevented this UD?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Nothing; Sandra should have known that the document was Top Secret and not shared it.
- ○ Ensure all proper markings are present on the document.

Classification

Now that we've discussed the classification markings required to identify and protect classified information, we're going to look at how those documents are classified. Effective classification processes protect against unauthorized disclosure. Misclassification may inadvertently lead to the disclosure of information that should be protected.

There are two ways information can be classified: original classification and derivative classification.

Original Classification

Original classification is the initial determination by an Original Classification Authority (OCA) that information needs protection because its disclosure could reasonably be expected to cause identifiable or describable damage to national security.

Derivative Classification

Derivative classification is incorporating, paraphrasing, restating, or generating in a new form information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information. The original source documents or a security classification guide (SCG) are the only authorized sources for derivative classification.

Declassification

Information must be declassified as soon as it no longer meets the standards for classification in accordance with regulatory guidance in E.O. 13526.

Declassification can occur through one of four systems.

- Automatic declassification occurs 25 years from the date of origin, whether or not the document has been reviewed, with the exceptions noted in E.O. 13526.
- Systematic declassification is a review of records of permanent historical value exempted from automatic declassification.
- Mandatory declassification occurs as a result of a request for review, if the information is not exempted, and if the information is not the subject of pending litigation.
- Finally, a declassification review will occur as a result of a request under the Freedom of Information Act (FOIA), Presidential Records Act, the Privacy Act of 1974, or a mandatory review.

Classification Activity

Now, check your knowledge. Jim is creating a new document that paraphrases Secret information from an authorized source document. What type of classification has occurred?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Original Classification
- ○ Paraphrased Classification
- ○ Declassification
- ○ Derivative Classification

Case Study: Bryan Martin

Remember, not properly protecting CNSI can lead to unauthorized disclosure and has real-life impacts. Let's take a look at a case study.

U.S. Navy Petty Officer second class, Bryan Martin, attempted to sell classified information, including photos, satellite images, and details about U.S. operations in Afghanistan and Iraq, to what he thought was a Chinese spy. In actuality, it was an undercover FBI agent.

This information was removed from secure facilities, which could have resulted in grave damage to national security.

CUI Requirements

CUI Access Intro

Let's turn our attention to CUI. The requirements for access to CUI are different than those for CNSI. Can you determine if someone is authorized to access CUI? Consider this scenario.

You are a human resources specialist. Your organization's health plan provider is asking for a roster of new personnel for enrollment in the plan, as elected by the personnel. In this situation, is the provider an authorized recipient? You'll have an opportunity to answer this question in a bit.

Requirements for Access to CUI

The standard requirement for individuals to access CUI is a lawful, government purpose. What is a lawful, government purpose? This includes any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes

as within the scope of its legal authorities or the legal authorities of non-executive branch entities.

CUI Access

Examples of groups of people who may have a lawful, government purpose as determined by the holder of the information:

- State and local law enforcement
- Congress
- State, local, tribal, and territorial governments
- Industrial partners
- Other federal agencies
- Allies and partner nations
- Members of academia

CUI Policy

Visit the policy guidance on CUI:

- E.O. 13556, Controlled Unclassified Information
- 32 CFR Part 2002, Controlled Unclassified Information
- DOD CUI Program
- DODI 5200.48, Controlled Unclassified Information
- 32 CFR Part 117, NISPOM Rule

CUI Access Activity

Remember the scenario we looked at earlier, in which a health plan provider asked you, an HR professional, for a roster of new personnel? In this situation, is the health plan provider an authorized recipient?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Yes, any administrator can access this information.
- ○ Yes, this is considered a lawful, government purpose.
- ○ No, only the human resources specialists are authorized.

Marking CUI Intro

Now that you understand who is authorized to access CUI, let's review the minimum marking requirements.

As with CNSI, UD of CUI can occur from improperly marked documents. Let's look at a scenario to see if you can prevent UD of CUI.

Your coworker, Judy, has created a new document that contains CUI. She has asked you to review the document to ensure she has marked it properly. Do you think it looks right? You will have the opportunity to check your answer after reviewing CUI marking requirements.

UNCLASSIFIED//FOUO

MEMORANDUM FOR XXXXXX

SUBJECT: CUI MARKINGS

When a document is designated as controlled unclassified information (CUI) the document must be clearly marked as such. This should include dissemination and decontrolling instructions.

Controlled by: OFFICE

Category: AS DESIGNATED

Distribution/Dissemination Control :

POC: Judy Sample (555)555-5555

UNCLASSIFIED//FOUO

Marking CUI

When an Unclassified document contains CUI, it must be clearly marked. The minimum DOD marking requirements for CUI are the acronym CUI in the banner and footer, and the Designation Indicator, (DI) block.

Portion markings are optional at this time, but if portion markings are used in the document, they must appear consistently in all sections.

To learn more about marking CUI, visit the course resources to access DODI 5200.48, DOD CUI Program, the DOD CUI Registry, and CDSE's CUI Life Cycle Shorts.

Marking CUI Activity

Time to check your understanding. Remember the scenario we discussed earlier? Here's a refresher.

Your coworker, Judy, has created a new document that contains CUI. She has asked you to review the document to ensure she has marked it properly. Is this properly marked?

UNCLASSIFIED//FOUO

MEMORANDUM FOR XXXXXX

SUBJECT: CUI MARKINGS

When a document is designated as controlled unclassified information (CUI) the document must be clearly marked as such. This should include dissemination and decontrolling instructions.

Controlled by: OFFICE

Category: AS DESIGNATED

Distribution/Dissemination Control :

POC: Judy Sample (555)555-5555

UNCLASSIFIED//FOUO

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Yes
- ○ No

Safeguarding CUI Intro

Now that you know who can access CUI and how to properly mark it, let's review CUI safeguarding.

Requirements for safely handling, transmitting, destroying, and decontrolling CUI are different than those for CNSI. Do you know how to protect CUI from UD?

Think of some methods of protection. After we review the safeguarding procedures, you'll have an opportunity to check your knowledge.

Safeguarding CUI

Let's learn what is required to protect CUI. You must safeguard CUI in a manner that minimizes risk of unauthorized disclosure and allows timely access to authorized holders, in accordance with DODI 5200.48. This instruction can be found in the resources section of this course.

Required measures for safeguarding CUI include the requirement to properly mark information designated as CUI in a controlled environment. To ensure no unauthorized individuals access CUI, always follow appropriate procedures for providing access to and sharing CUI.

When CUI needs to be destroyed or decontrolled, ensure you are following the procedures in regulatory guidance. When the information designated as CUI no longer needs safeguarding and when permitted by applicable laws and regulations, decontrol the CUI. Note that decontrolling CUI does not mean that it is authorized for public release. This will be discussed in more detail in a later lesson.

Protecting CUI Activity

Let's practice safeguarding CUI. Consider this scenario.

During your duty day, you are working with CUI. It is your responsibility to ensure it is protected. What are some ways you can help to protect CUI?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Ask a coworker to watch your desk if you need to get up.
- ☐ Do not share your screen with others.
- ☐ Maintain physical and visual control.
- ☐ Use SF 901 coversheet when carrying or transporting.

Transmitting CUI Activity

Next, while you are working with CUI on a properly accredited information system , your coworker, Jack, asks you to provide him the document for an authorized government purpose. How can you safely transmit this CUI to Jack?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Send via fax to his main office fax number.
- ☐ Send it as an encrypted email via your government email.
- ☐ Scan the document and send via your cell phone.
- ☐ Send it using DOD SAFE.

Storing CUI Activity

You have made it to the end of your duty day and are ready to go home. You have printed CUI in your possession, and you work in a facility without continuous monitoring. How can you safely store this CUI at the end of the day to protect against UD?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Take it home for safekeeping.
- ○ Leave it on your desk with a cover page.
- ○ Lock it in your desk drawer.

Case Study: OPM Data Breach

Unauthorized disclosure of CUI can have a serious adverse effect on organizations and individuals. One incident that had a significant impact on national security and to the affected personnel’s lives occurred in April 2015.

In this case, the Office of Personnel Management (OPM) reported a significant CUI incident that occurred. In this incident, personnel records, comprised of Personally Identifiable Information (PII), and Protected Health Information (PHI) were compromised. The personnel files of 4.2 million former and current government employees were compromised, and it included a breach of 21.5 million security clearance background investigations.

While approximately 600,000 individuals were impacted solely by the personnel records incident, a total of approximately 3.6 million individuals were impacted by both the personnel records and background investigation incidents. In total, 5.6 million individuals had their fingerprint data stolen.

Through this data breach, many individuals were impacted. The data contained PII and PHI, some of which could be embarrassing to individuals. This compromised data breach provided intelligence and counterintelligence value to foreign adversaries, and in total, the government expense to notify and protect affected individuals was $350 million.

Conclusion

Lesson Summary

You have completed the *Life Cycle Protection Requirements* lesson.

Lesson 4: Security and Policy Reviews

Introduction

Introduction

Welcome to the Security and Policy Reviews lesson. This lesson will provide you with prepublication review requirements and review the role of the Public Affairs Office (PAO) in protecting national security information against unauthorized disclosure.

Take a moment to review the lesson objectives.

- Given a scenario, apply DOD policy requirements to protect CNSI and CUI from unauthorized disclosure.
  - Given a scenario, determine prepublication review requirements for national security information.
  - Given a scenario, determine the role the Public Affairs Office (PAO) serves to protect against unauthorized disclosure.

Security and Policy Reviews

Security and Policy Review Introduction

You have learned how to safeguard classified information, but some information *does* need to be shared or published. Do you know how to ensure you don't inadvertently disclose information that should *not* be shared?

Let's review this scenario. You are preparing to give a speech that includes details about your DOD service and related information. You are retired and no longer work for a DOD agency. Do you know what you need to do to protect against unauthorized disclosure before delivering your speech?

Let's consider the process for releasing information to the public.

Prepublication Requirements

In the scenario you just reviewed, you wrote a speech that contained information related to your time working in the DOD. This speech will require a prepublication review. Let's take a deeper look into the reasons why this is a requirement.

People who have had access to classified national security information (CNSI), controlled Unclassified information (CUI), or non-public DOD information may be in a position to write books, articles, speeches, briefings, and more. If these writings include any DOD information, they must be submitted for a prepublication review before public release, to minimize the risk of unauthorized disclosure.

Public release includes, but is not limited to sending any book, manuscript, or article to a publisher, editor, movie producer, or game purveyor. It also includes delivering or sharing any speech, briefing, article, or content in any form that will be publicly available. This requirement applies to past and present government civilian employees, contractor personnel, military personnel, and retirees.

There are two offices that may be involved in determining whether information may be publicly released. These are the Defense Office of Prepublication and Security Review (DOPSR) and the organization or Component public affairs office (PAO).

You will learn more about these in this lesson.

DOPSR

Role of DOPSR

So, what is DOPSR's role? DOPSR manages the DOD security review program, reviewing written materials both for public and controlled release under the authority of DOD Instruction (DODI) 5230.09, Clearance of DOD Information for Public Release, and DODI 5230.29, Security and Policy Review of DOD Information for Public Release.

DOPSR conducts prepublication reviews to ensure information that could be damaging to national security is not disclosed. During this process, they will examine the information proposed for public release for two purposes. DOPSR reviews the information to ensure compliance with established national and DOD policies, as well as to determine whether it contains any classified, CUI, or Unclassified information that may, individually or in compilation, lead to the compromise of classified information or compromise national or operational security.

However, note that DOPSR does not review resumes or cover letters, even though military members and federal civilian employees often work in special programs. As a best practice, your current or last command can conduct a security review of these documents.

DOPSR Reviews

The originating DOD office is responsible for ensuring prepublication review occurs and that the information is "cleared" before releasing information to the public. DOD

components are responsible for the initial security and policy reviews of any information prepared for or by their DOD personnel that is intended for public release. DOD component heads are required to establish policies and procedures to implement a prepublication review process and send details about the review process to DOPSR.

The course resources provide additional information, including DODI 5230.09, 5230.29, and the DOPSR Prepublication Brochure, which details what information to submit, where to submit it, and submission timelines.

PAO

PAO Function

Before we review the role of the PAO in the security and policy review process, let's first review the overall role of the PAO. Often DOD component senior leadership delegate the responsibility of releasing information to the public to the PAO.

The PAO performs a variety of functions, including researching, planning, budgeting, executing, and evaluating operations that involve the public. This includes first ensuring information is authorized for release. It also involves liaising with the news media and ensuring information and communications support agency goals and promote public trust in the agency. The PAO also communicates timely, truthful, accurate, and credible information to a variety of audiences.

PAO Role in Releasing Information

So, what role does the PAO play in the security review process?

When applicable, the PAO may coordinate the process for releasing information or support the local command throughout the process. First, the local or command security manager conducts a security and policy review. If it is determined that content is related to other DOD components and U.S. government agencies; it would then need to be submitted for a DOPSR review. The PAO may also be responsible for conducting a public affairs review. These reviews focus on specific considerations such as ensuring political views are not portrayed or ensuring information that could discredit the military or federal government is avoided. These reviews also help to protect against other offensive views being promoted.

All of these actions help to mitigate risk before releasing information to the public. This PAO review is outside of, and in addition to reviews that protect CNSI or CUI from unauthorized disclosure.

Security and Policy Review Activity 1

Let's get back to the scenario. As a reminder, you are preparing to give a speech that includes details about your DOD service and related information. You know that you need to send it for a prepublication review through DOPSR. What will they review the speech for?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Ensure compliance with established national and DOD policies
- ☐ Ensure political views are not portrayed
- ☐ Protect against offensive views being portrayed
- ☐ Ensure there is no information that may compromise classified information

Security and Policy Review Activity 2

After the DOPSR review of your speech is complete, the PAO, on behalf of the DOD agency you worked for, reviews your speech. How will the PAO determine if your speech can be released to the public?

Select all that apply. Check your answer in the Answer Key at the end of this Student Guide.

- ☐ Ensure information that could discredit the military or federal government is avoided
- ☐ Ensure political views are not portrayed
- ☐ Protect against offensive views being portrayed
- ☐ Ensure there is no information that may compromise classified information

Conclusion

Lesson Summary

You have completed the *Security and Policy Reviews* lesson.

Lesson 5: Social Media Policy

Introduction

Lesson Overview

Welcome to the *Social Media Policy* lesson. Social media guidelines within the Department of Defense (DOD) exist to protect DOD networking services and regulate the personal use of social media in a DOD environment. In this lesson, you will learn these requirements to ensure you follow procedures for using social media platforms.

Take a moment to review the lesson objectives.

- Given a scenario, apply DOD policy requirements to protect CNSI and CUI from unauthorized disclosure.
    - Given a scenario, apply DOD policy requirements to authorized and unauthorized use of social media.

Social Media Guidelines

Social Media Introduction

Are you aware of the DOD policy regulations in place for using social media? Social media services include, but are not limited to:

- Facebook
- X, formerly known as Twitter
- YouTube
- LinkedIn
- Wikis
- Instagram
- Threads
- TikTok
- Blogs

Certain social media applications, such as TikTok, are prohibited on all government information systems and devices. The “No TikTok on Government Devices Act”, which went into effect in December of 2022, specifically prohibits the TikTok platform.

Additionally, all non-public DOD information is prohibited on any electronic messaging service not controlled by the DOD, per a Secretary of Defense Memo issued in April of 2023 on the "Immediate Review and Assessment of DOD Information Security Programs." This includes private social media accounts or groups as well as any messaging apps that may appear to be protected or encrypted, such as WhatsApp and Signal.

Posting on Social Media

Social media has become a large part of many people's lives. As a DOD employee or contractor, you are not prohibited from posting on social media, but you need to exercise discretion in what you choose to post. Do you know what is acceptable to post and what isn't? You may want to post a picture of your dog, the office where you're working, pictures from your family vacation, or keep your friends and family updated on where you will be during your deployment.

Which of these is safe to post and which isn't? You'll learn the guidelines next, then have the opportunity to test your knowledge.

Guiding Publications

As you just learned, not all social media posts are prohibited, but you need to be aware of what you're posting.

DOD Instruction (DODI) 5400.17, Official Use of Social Media for Public Affairs Purposes, states that DOD personnel are permitted to use unofficial personal social media, within guidelines. These guidelines are intended to prevent the unauthorized disclosure of non-public DOD information or Unclassified information that can aggregate to reveal classified information or the appearance of DOD endorsement or sanction of personal opinions.

Remember, if in doubt, it's best not to post on social media accounts or send non-public DOD information via a private messaging app, whether or not it's encrypted or appears to be secure. What you see here, what you do here, when you leave here, it stays here.

DODI 5400.17

DODI 5400.17, Official Use of Social Media for Public Affairs Purposes, prohibits DOD personnel from disclosing non-public information to promote their private interests or the private interests of others. Additionally, DOD personnel must adhere to all operations security and unit-level directives, including forward-operating environments.

It is important to remember that releasing unauthorized content through any means, including social media, may unnecessarily endanger or compromise individuals, units, and the mission. You must always be mindful of your obligation to protect classified national security information (CNSI) and controlled Unclassified information (CUI) to prevent unauthorized disclosure.

DODM 5200.01, Volume 3

DOD Manual (DODM) 5200.01, Volume 3, DOD Information Security Program: Protection of Classified Information, provides dissemination requirements for protection of classified information. Note that these same dissemination requirements apply when you are sharing information on social networking services. Penalties for ignoring the requirements are likewise the same.

DODI 5200.48

DODI 5200.48, Controlled Unclassified Information, outlines requirements for protecting CUI. It requires that the DOD originator or authorized CUI holder ensure a prepublication security and policy review is conducted, pursuant to the standard DOD Component process, before CUI is approved for public release. This includes publication to a publicly available website.

DODI 8170.01

DODI 8170.01, Online Information Management and Electronic Messaging, outlines requirements for managing information online and through electronic messaging. It establishes policies for initiating an external official presence on approved social media platforms.

The Office of the Secretary of Defense (OSD) and DOD Components must assess the communication value to provide timely and accurate information to the public and the media. Information that is being released must be carefully considered and avoided unless it meets a specific communications objective that is not being met otherwise.

Posting on Social Media Activity 1

Let's check your understanding. Can you determine what is safe to put on social media and what should not be posted? Is it safe to post a picture of a dog you saw outside the base?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Post

- ○ Delete

Posting on Social Media Activity 2

Next, you want to post an image of the DOD installation where you're working for your current detail. Is it safe to post the image of the DOD installation?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Post
- ○ Delete

Posting on Social Media Activity 3

You just got back from vacation and want to post pictures from the trip. Are these safe to post?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Post
- ○ Delete

Posting on Social Media Activity 4

Finally, you just found out details about an upcoming deployment and you want to let your friends and family know you'll be gone. Is this safe to post?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Post
- ○ Delete

Case Study: Henry Frese

Now that we've reviewed the regulations surrounding the use of social media to protect against unauthorized disclosure, let's look at a real-life case that involved unauthorized disclosure via social media.

Henry Frese, a former Defense Intelligence Agency (DIA) analyst, held Top Secret/Sensitive Compartmented Information (TS/SCI) clearance. In October 2019, Frese was arrested for disclosing National Defense Information (NDI) to several journalists and a foreign consultant without authorization. He communicated with and transferred information to these individuals via Twitter for personal gain.

Conclusion

Lesson Summary

You have completed the *Social Media Policy* lesson.

Lesson 6: Reporting and Sanctions

Introduction

Lesson Introduction

Welcome to the *Reporting and Sanctions* lesson. The prevention of serious security incidents such as unauthorized disclosure is a responsibility shared by all Department of Defense (DOD) personnel. It is critical to be able to identify and report these incidents when they occur.

In this lesson, you will learn how to respond to and report unauthorized disclosure, or UD, along with the sanctions that result from a UD incident.

Take a moment to review the lesson objectives.

- Given a scenario, determine the required steps for reporting an unauthorized disclosure.
  - Given a scenario, respond appropriately to CNSI or CUI appearing in the public domain.
  - Given a scenario, identify the steps for reporting a specific unauthorized disclosure.
  - Given an example, identify sanctions that may be brought against someone who fails to protect CNSI and CUI.

Information Appearing in the Public Domain

Responding to Unauthorized Disclosure

How will you react when you encounter UD in your daily duties?

You may be approached about information that appears in the public domain. Your response to a potential UD incident can help prevent a critical national security incident. Here's a scenario of a potential UD incident you may experience.

You receive an email from a journalist with a national publication, asking you for a comment about the range of a new missile. Think about how you might respond to the email while you review the process for handling incidents appearing in the media. You'll get a chance to test your response once you learn the process.

Information in the Media

Information appearing in the public media is a serious matter, and at times you may be approached by a member of the media, as in the scenario about the journalist seeking information about a missile.

To properly address the serious issue of information appearing in the media, you should not make any statement that confirms or denies the accuracy of national security information. Instead, report it directly to your security manager or follow Component-specific guidance.

Responding to Unauthorized Disclosure Activity

Remember the scenario we discussed earlier? Now's your chance to decide how to handle it.

You receive an email from a journalist with a national publication, asking you for a comment about the range of a new missile. What should you do with this email?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Reply with Comment
- ○ Reply and CC Security Manager
- ○ Report to Security Manager

Reporting Steps

Reporting UD

You now know how to handle requests that come from the media, but do you know the required steps to take if classified information isn't properly safeguarded in your workplace? Let's review what to do if you find classified information in an unauthorized area.

While walking through the hall, you are stopped by a coworker, John, who tells you he found Top Secret documents in the bathroom. Do you know what to do in this instance?

Keep this scenario in mind as we review the reporting steps. You'll get to test your knowledge after reviewing the reporting process.

Reporting Steps 1 and 2

Let's review the reporting steps using an example.

First, meet Laura, a civilian employee working for the DOD. Laura has eligibility, access, and a need-to-know for Secret level information. One morning, Laura is working on her Unclassified system, a Non-Classified Internet Protocol Router (NIPR). While working on a shared network drive and reviewing resources for a project, she discovers a document saved in one of the network drive folders. Upon further inspection, she realizes the document she found is classified Secret and should not be on the NIPR shared drive. Laura makes note of where she found the file, does not forward or manipulate the file, and secures the area.

Laura has completed step one of the reporting process: Safeguarding Information. As you have learned throughout this course, properly safeguarding CNSI requires securing it by placing it in a General Services Administration (GSA) approved security container or other approved method for safeguarding or securing an area after spillage occurs. Remember, safeguarding CNSI requires that you minimize risk of UD.

Returning to our example, Laura takes her note of where she found the file and immediately goes to her security manager to report the UD.

Laura has performed step two of the reporting process: Report. When you suspect UD, you should report it to your Security Manager or Facility Security Officer (FSO) immediately after safeguarding. The FSO or Security Manager will report it to authorities at the next level.

Reporting Steps 3 and 4

So far, we have learned about the first two steps of the reporting process: Safeguard and Report. Let’s get back to the scenario to learn about the next steps in the process.

Laura notifies her Security Manager of the security incident, which she believed was spillage. In her report to the Security Manager, she included where and when she discovered the document, and any other details the Security Manager requested.

The Security Manager reports the incident to the appropriate Original Classification Authority (OCA) to initiate an initial classification review and a damage assessment. The Security Manager will coordinate with appropriate leadership, the appointment of an inquiry officer to conduct an inquiry into the potential spillage.

The officer conducting the inquiry, Sophie, interviews the original author, Zach, who created the file. Zach believed that the information he included in the file was Unclassified; however, upon further inspection of the source document, Zach concluded that the information he used was indeed classified Secret. While drafting

the report, Zach included a Secret banner marking in his report, which prompted Laura to report the document upon discovery.

During the inquiry, the incident response center also identified that the file was only located in one place on the network and a copy was also on Zach's local desktop. Additionally, by coordinating with the responsible incident response center, the officer conducting the inquiry discovers that five other employees had accessed the file. Sophie verifies the clearance level and need-to-know of the five individuals and discovers that three of the five personnel who accessed the file do not have the appropriate eligibility level or need-to- know to access the information contained in the document involved in the spillage.

The actions described represent step three: Inquire. The appointed inquiry officer leads the inquiry process for the incident.

The inquiry officer has sufficiently addressed all of the questions and determines that further investigation is not necessary. Step four in the reporting process, Investigate, is conducted when an inquiry does not yield answers to all of the questions required. Our scenario does not warrant further investigation.

Reporting Steps 5 and 6

Let's review what we know about the UD reporting process so far.

- In step one, the information is safeguarded.
- In step two, the potential UD is reported.
- During step three, an inquiry into the potential UD is conducted.
- In step four, an investigation may occur, if the initial inquiry leaves unanswered questions.

Let's move on to the next steps by revisiting our scenario.

The inquiry clearly revealed that spillage had occurred and classified information was compromised, which is a security violation. Classified information was discovered on a NIPR shared drive. In this instance, classified information was stored and processed on an Unclassified network. Additionally, classified information was shared and disclosed to three individuals who did not have a valid clearance, authorized access, or a need to know.

This represents step five of the reporting process: Evaluate, in which the results of the inquiry and, if necessary, the investigation, are evaluated to determine if the incident is a security infraction or a security violation. It also may involve evaluating the severity of the UD in situations where loss or compromise has occurred.

In step six: Elevate, the results of the incident are elevated in accordance with policy. DOD UD additional reporting depends on the category of information that has been compromised.

With spillage as we have in this scenario, at minimum, you would need to notify the OCA and the Information System Security Manager (ISSM). In some situations, results of the inquiry and investigation may need to be elevated to the UD Program Management Office (PMO) and the appropriate Military Department Counterintelligence Organizations (MDCOs).

For more information on elevating results when required, reference the course resources for job aids: How to Respond to UD of Classified and CUI and the DOD Unauthorized Disclosure Desk Reference.

Reporting Steps 7 and 8

So far, we have learned about six of the eight steps of the reporting process for UD: Safeguard, Report, Inquire, Investigate, Evaluate, and Elevate. Let's get back to the scenario to learn about the final two steps.

As the incident of spillage led to a confirmed incident of unauthorized disclosure, different courses of action could be implemented to mitigate the risk of further unauthorized disclosures. For personnel who read and did not report the spillage that was discovered during the audit of the shared drive path and file modification and access logs, those personnel are now required to complete their Cyber Awareness Challenge and more in-depth Unauthorized Disclosure training on proper usage of IT systems and their reporting requirements. Additionally, the office where the personnel involved in the incident work launched a security awareness campaign with the agency to help reduce future incidents of spillage.

This represents step seven of the UD reporting process: Correct. In step seven, corrective actions should be implemented that focus on preventing future incidents and eliminating any conditions that might have contributed to the event. The cognizant DOD Component will determine and implement the appropriate corrective actions based on the extent or severity of the incident.

Finally, in this scenario the DOD Component head issued a warning to the personnel found responsible for the UD incident.

This represents step eight: Sanction, in which the individuals responsible for the incident may be subject to criminal or administrative sanctions in accordance with regulatory guidance. These include instituting any administrative actions as outlined in DODM 5200.01, Volume 1. Administrative sanctions include a warning, reprimand, and suspension without pay. Criminal sanctions must be undertaken when

applicable, in accordance with the Uniform Code of Military Justice or sections 801 to 940 of Title 10, U.S.C.

Reporting Steps Review

You have now learned about the eight reporting steps when you encounter UD:

- Safeguard
- Report
- Inquire
- Investigate
- Evaluate
- Elevate
- Correct
- Sanction

The first two steps of the process apply to everyone. They are essential and the responsibility of anyone who believes they have witnessed, discovered, or have knowledge of an unauthorized disclosure. Refer to the course resources for the job aid “How to Respond to UD of Classified Information and CUI” which will guide you through steps in the reporting process.

Step 1: Safeguard

Step one is to safeguard the information. It is your responsibility to complete this step should you encounter an instance of UD.

Step 2: Report

Step two is to report the unauthorized disclosure. You should report it to your Security Manager or Facility Security Officer, or FSO, immediately after safeguarding. The FSO or security manager will report it to authorities at the next level. This step is completed by the individual who discovers the UD.

Step 3: Inquire

In step three, the appointed inquiry officer will lead the inquiry process for the incident.

Step 4: Investigate

In step four, the incident will be investigated by the appointed inquiry officer, if applicable.

Step 5: Evaluate

In step five, the results of the inquiry/investigation will be evaluated to determine severity and if a security infraction or a security violation occurred.

Step 6: Elevate

In step six, based on the results of the evaluation and the category of information, elevate the results as required. At minimum, notify the OCA when loss or compromise of classified has occurred so a damage assessment can be initiated.

Step 7: Correct

In step seven, corrective actions should be implemented that focus on preventing future incidents and eliminating any conditions that might have contributed to the event. The cognizant DOD Component will determine and implement the appropriate corrective actions based on the extent or severity of the incident.

Step 8: Sanction

In step eight, the individuals responsible for the incident may be subject to criminal, civil, or administrative sanctions in accordance with regulatory guidance.

Security Manager Reporting Requirements

As an FSO or Security Manager, you have the additional responsibility of reporting any unauthorized disclosures to the appropriate authorities.

Requirements for handling UD are different for CNSI and CUI. Personally identifiable information, or PII—which is a type of CUI—has additional requirements as well. Unique handling considerations and additional reporting requirements are typically involved with the unauthorized disclosure of special categories of CNSI or CUI or when specific circumstances surround a UD.

Refer to the course resources for a downloadable job aid “How to Respond to UD of Classified and CUI” to see which steps apply directly to you or your personnel.

CNSI

If the unauthorized disclosure involved CNSI, you must report it to the Original Classification Authority (OCA) to conduct a damage assessment; this may vary depending on if you are an FSO or DOD Security Manager.

UD of certain types of classified information or specific circumstances requires unique handling or additional reporting requirements. Reference DODM 5200.01 Vol. 3 enclosure 6.

CUI

When CUI is released in the public domain without authorization, you must notify the Security Manager and the Unauthorized Disclosure Program Management Office (UD PMO) immediately.

PII

For PII, which is a type of CUI, you may need to report to an additional office, depending on if you are a DOD Security Manager or FSO. These offices include:

- U.S. Cyber Command (USCYBERCOM)
- U.S. Computer Emergency Readiness Team
- Your DOD Component head
- DOD Privacy Act officials
- UD PMO
- Military Department Counterintelligence Organization

Reporting Activity

Review the scenario where your coworker approaches with Top Secret documents he found in the bathroom. Knowing the reporting steps, what should you do next?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Ask them to shred it
- ○ Safeguard it and report it to your Security Manager
- ○ Tell them to report it
- ○ Safeguard it and tell them not to say anything

Sanctions

Sanctions

Are you aware of the types of sanctions that could be imposed in relation to unauthorized disclosure? The last step of the reporting process involves imposing sanctions if applicable. Criminal, civil, and/or administrative sanctions may be brought against an individual who fails to protect CNSI or CUI.

Think back to the case studies from throughout this course. What sanctions do you think applied to them? We'll review that next.

Case Study Recap

In the cases we have reviewed in this course, each perpetrator received sanctions for their actions.

- Daniel Hale pleaded guilty to retention and transmission of national defense information, or NDI. He was sentenced to 45 months in federal prison.
- Bryan Martin pleaded guilty to four counts of attempted espionage. He was sentenced to 34 years in prison, was reduced in rank, forfeited all pay and allowances, and was dishonorably discharged from the Navy.
- Henry Frese pleaded guilty to the willful transmission of Top Secret NDI and was sentenced to 30 months in prison.

Conclusion

Lesson Summary

You have completed the *Reporting and Sanctions* lesson.

Lesson 7: Course Completion

Course Summary

Summary

In this course, you learned how to identify, prevent, and report unauthorized disclosure incidents. Remember, unauthorized disclosure can put national security at risk. It's up to you to remain vigilant in preventing unauthorized disclosure.

Course Summary

Congratulations! You have completed the *Unauthorized Disclosure of Classified Information and Controlled Unclassified Information* course.

You should now be able to perform all of the listed activities.

- Given a scenario, assess whether an action is an unauthorized disclosure of CNSI or CUI.
- Given a scenario, apply DOD policy requirements to protect CNSI and CUI from unauthorized disclosure.
- Given a scenario, determine the required steps for reporting an unauthorized disclosure.

To receive course credit, you must take the *Unauthorized Disclosure of Classified Information and Controlled Unclassified Information* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to access the online exam.

Appendix A: Answer Key

Lesson 2 Activities

UD Type Activity

Example 1 of 4. Lily has access to Top Secret information. She is selected to do an interview about her role within the DOD and during the interview, she discloses Top Secret program information. The journalist who interviewed her publishes the information. What type of UD is this?

- ○ Spillage
- ⦿ Public domain (correct response)
- ○ Espionage
- ○ Improper safeguarding

Feedback*: This is an example of a public domain UD.*

Example 2 of 4. Ted is working with a potential DOD contractor for a new project. The contractor asks Ted for CUI related to the contract, and Ted sends the CUI from his DOD Information System via unencrypted email. What type of UD is this?

- ⦿ Spillage (correct response)
- ○ Public domain
- ○ Espionage
- ○ Improper safeguarding

Feedback: *This is an example of spillage.*

Example 3 of 4. Erin works as a defense intelligence analyst studying a near peer country's drone production. She works closely with allied foreign partner analysts, but always on separate problem sets. One of the allied analysts in particular, Jerome, concentrates on the near peer's government equities, but has lately been asking Erin a lot of questions regarding the country’s drone capabilities - which is outside his problem set. Jerome does not have a need-to-know but is very persistent. What type of UD is this?

- ○ Spillage
- ○ Public domain
- ⦿ Espionage (correct response)
- ○ Improper safeguarding

Feedback: This is an example of espionage.

Example 4 of 4. While working with paper copies of Secret information, Marshall leaves the secure area to use the restroom. He leaves the Secret documents on the restroom counter, and they are later discovered by an uncleared facility custodian. What type of UD is this?

- ○ Spillage
- ○ Public domain
- ○ Espionage
- ⊙ Improper safeguarding (correct response)

Feedback: *This is an example of improper safeguarding.*

Misconceptions Activity

Check your understanding of UD misconceptions. Which of these is a misconception related to UD?

- ☑ It is okay to read, discuss, and freely share CNSI or CUI that has been put in the public domain. (correct response)
- ☑ You may receive protection through "journalist privilege" if you disclose CNSI or CUI to a journalist. (correct response)
- ☑ Manuscripts, books, etc., can be submitted to an editor or publisher before undergoing a security review. (correct response)
- ☑ Once I leave my organization, the SF 312 NDA no longer applies. (correct response)
- ☑ It is okay to share Unclassified DOD information on a "secure" messaging app. (correct response)

Feedback: *All of these are misconceptions about sharing CNSI or CUI.*

Whistleblowing Activity

Let's revisit the scenario we introduced earlier. Can you determine whether or not it is whistleblowing? Remember, in this scenario an insider believes the government poses a danger to the public and releases national security information on a social networking site to make the public aware of the danger. Is this whistleblowing or unauthorized disclosure?

- ○ Whistleblowing
- ⊙ Unauthorized Disclosure (correct response)

Feedback: *Posting protected national security information in the public domain is unauthorized disclosure.*

Damage Activity

Let's revisit the scenario we introduced you to earlier. Do you know the correct response?

While you are scrolling social media, you happen to see a post from one of your coworkers. This coworker has disclosed CUI on their private social media account: "Check out this upcoming draft DOD policy I was asked to review this week – can you believe these changes?" Can this disclosure result in damage?

- ⦿ Flag post – this can cause damage (correct response)
- ○ No issue – the information isn't classified

Feedback: *Even disclosing nonpublic DOD Unclassified and CUI can cause damage. Also, keep in mind that nonpublic Unclassified information and CUI can be aggregated to reveal classified information, damaging national security.*

Lesson 3 Activities

Access Activity

You have control of Secret CNSI for a project you are managing. You receive a request from Andrew, who holds eligibility at the appropriate security level and has signed an SF 312 for the CNSI you control. Should you give Andrew access to the CNSI?

- ○ Yes, since he has signed an SF 312 and possesses eligibility, he is eligible to access classified information.
- ⦿ No, he must also have a "need-to-know" to access classified information. (correct response)
- ○ No, he must have Top Secret eligibility in order to access classified information.
- ○ No, he must have a signed order from his superior in order to access classified information.

Feedback: *It is not simply eligibility at the appropriate level and signed SF 312 that allows an individual to access classified information. That individual also must have a "need-to-know" for that classified information.*

Safeguarding CNSI Activity 1

You are working with paper copies of Top Secret information to prepare for an upcoming brief. While you walk from your desk to the briefing room, you want to ensure that no one can view the information who does not have access to it. In this situation, how would you protect it?

- ○ Protect it in a manila folder
- ⊙ Use an SF 703 cover sheet (correct response)
- ○ Print a watermark identifying it as CNSI
- ○ Mark “Working Paper” on the first page

Feedback*: It is required to protect printed copies of Top Secret information by using an SF 703 cover sheet.*

Safeguarding CNSI Activity 2

Next, you receive a request from a co-worker, Bianca, who is authorized to access the Secret information that you possess for a project she is working on. She is located in an office across the country from you. In this situation, how would you safely transmit the CNSI to Bianca?

- ○ Send it encrypted via an Unclassified email and request a read receipt
- ⊙ Send it on a properly accredited system via secure email after ensuring that Bianca has an accredited Secret level system (correct response)
- ○ Send it via any commercial shipping service after ensuring Bianca can store it properly
- ○ Call Bianca on your work cell phone to share the critical information

Feedback: *There are a few ways to transmit CNSI. In this instance, you can send Bianca the Secret information on a properly accredited system using a secure properly marked email after ensuring that Bianca has access to a system accredited at the appropriate level.*

Safeguarding CNSI Activity 3

You have been handling Secret information for a classified project you are working on all day and are ready to head home. In this situation, how would you safely store the CNSI before heading home, given that your work location does not have an approved open storage area?

- ○ Place it in a locked desk drawer
- ⊙ Place it in a GSA-approved container (correct response)

- ○ Place it in a properly marked folder on your desk
- ○ Give it to your supervisor for safekeeping

Feedback: *In order to safely store Secret information in an area that is not approved for open storage you must place it in a GSA-approved container or vault when not in use.*

Marking CNSI Activity

UNCLASSIFIED//FOUO

MEMORANDUM FOR XXXXXX

SUBJECT: CUI MARKINGS

When a document is designated as controlled unclassified information (CUI) the document must be clearly marked as such. This should include dissemination and decontrolling instructions.

Controlled by: OFFICE

Category: AS DESIGNATED

Distribution/Dissemination Control :

POC: Judy Sample (555)555-5555

UNCLASSIFIED//FOUO

Sandra shared this document, which contains Top Secret information, with a colleague who does not hold Top Secret eligibility. What could have prevented this UD?

- ○ Nothing; Sandra should have known that the document was Top Secret and not shared it.
- ⊙ Ensure all proper markings are present on the document. (correct response)

Feedback: *There should be a TOP SECRET marking in the header which alerts the holder to the presence of CNSI.*

Classification Activity

Now, check your knowledge. Jim is creating a new document that paraphrases Secret information from an authorized source document. What type of classification has occurred?

- ○ Original Classification
- ○ Paraphrased Classification
- ○ Declassification
- ⊙ Derivative Classification (correct response)

Feedback: *Derivative classification occurs when incorporating, paraphrasing, restating, or generating in a new form information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information.*

CUI Access Activity

Remember the scenario we looked at earlier, in which a health plan provider asked you, an HR professional, for a roster of new personnel? In this situation, is the health plan provider an authorized recipient?

- ○ Yes, any administrator can access this information.
- ⊙ Yes, this is considered a lawful, government purpose. (correct response)
- ○ No, only the human resources specialists are authorized.

Feedback: *The standard for access to CUI, like a personnel roster, is a lawful government purpose.*

Marking CUI Activity

UNCLASSIFIED//FOUO

MEMORANDUM FOR XXXXXX

SUBJECT: CUI MARKINGS

When a document is designated as controlled unclassified information (CUI) the document must be clearly marked as such. This should include dissemination and decontrolling instructions.

Controlled by: OFFICE

Category: AS DESIGNATED

Distribution/Dissemination Control :

POC: Judy Sample (555)555-5555

UNCLASSIFIED//FOUO

Your coworker, Judy, has created a new document that contains CUI. She has asked you to review the document to ensure she has marked it properly. Is this properly marked?

- ○ Yes
- ⊙ No (correct response)

Feedback: *This document is marked FOUO, which is a legacy marking. This document should be assessed to see if it meets criteria for CUI and marked appropriately. Judy should review the DOD CUI Registry to determine if the information aligns with one of the CUI categories.*

Protecting CUI Activity

During your duty day, you are working with CUI. It is your responsibility to ensure it is protected. What are some ways you can help to protect CUI?

- ☐ Ask a coworker to watch your desk if you need to get up.
- ☑ Do not share your screen with others. (correct response)
- ☑ Maintain physical and visual control. (correct response)
- ☑ Use SF 901 coversheet when carrying or transporting. (correct response)

Feedback**:** *Remember to maintain physical and visual control of the CUI. When carrying or transporting CUI, as a best practice, use SF 901 coversheet.*

Transmitting CUI Activity

Next, while you are working with CUI on a properly accredited information system , your coworker, Jack, asks you to provide him the document for an authorized government purpose. How can you safely transmit this CUI to Jack?

- ☐ Send via fax to his main office fax number.
- ☑ Send it as an encrypted email via your government email. (correct response)
- ☐ Scan the document and send via your cell phone.
- ☑ Send it using DOD SAFE. (correct response)

Feedback**:** *To safely transmit CUI, it is best practice to send it as an encrypted email using your government email. Another method for safely transmitting CUI is through DOD SAFE.*

Storing CUI Activity

You have made it to the end of your duty day and are ready to go home. You have printed CUI in your possession, and you work in a facility without continuous monitoring. How can you safely store this CUI at the end of the day to protect against UD?

- ○ Take it home for safekeeping.
- ○ Leave it on your desk with a cover page.
- ⊙ Lock it in your desk drawer. (correct response)

Feedback**:** *You can safely store the CUI by locking it in your desk drawer overnight to protect it from UD.*

Lesson 4 Activities

Security and Policy Review Activity 1

Let’s get back to the scenario. As a reminder, you are preparing to give a speech that includes details about your DOD service and related information. You know that you need to send it for a prepublication review through DOPSR. What will they review the speech for?

- ☑ Ensure compliance with established national and DOD policies (correct response)
- ☐ Ensure political views are not portrayed

- ☐ Protect against offensive views being portrayed
- ☑ Ensure there is no information that may compromise classified information (correct response)

Feedback: *DOPSR reviews seek to ensure compliance with established national and DOD policies and that there is no information that may lead to unauthorized disclosure of classified information or compromise national or operational security.*

Security and Policy Review Activity 2

After the DOPSR review of your speech is complete, the PAO, on behalf of the DOD agency you worked for, reviews your speech. How will the PAO determine if your speech can be released to the public ?

- ☑ Ensure information that could discredit the military or federal government is avoided (correct response)
- ☑ Ensure political views are not portrayed (correct response)
- ☑ Protect against offensive views being portrayed (correct response)
- ☐ Ensure there is no information that may compromise classified information

Feedback**:** *PAO reviews help ensure information is not included that could discredit the military or federal government. They also ensure political views or controversial views are not portrayed.*

Lesson 5 Activities

Posting on Social Media Activity 1

Let’s check your understanding. Can you determine what is safe to put on social media and what should not be posted? Is it safe to post a picture of a dog you saw outside the base?

- ⦿ Post (correct response)
- ○ Delete

Feedback**:** *This image does not contain any information related to the DOD and does not include any sensitive information. It is safe to share.*

Posting on Social Media Activity 2

Next, you want to post an image of the DOD installation where you’re working for your current detail. Is it safe to post the image of the DOD installation?

- ○ Post

⊙ Delete (correct response)

Feedback**:** *Remember, posting information related to the DOD that has not been cleared for public release on social media is prohibited. In this case, posting specific information about a DOD installation where you're working is not safe to post on social media.*

Posting on Social Media Activity 3

You just got back from vacation and want to post pictures from the trip. Are these safe to post?

⊙ Post (correct response)
○ Delete

Feedback: *While it is a best practice to wait until after a vacation to share details about the vacation, it is safe to post about it after you return.*

Posting on Social Media Activity 4

Finally, you just found out details about an upcoming deployment and you want to let your friends and family know you'll be gone. Is this safe to post?

○ Post
⊙ Delete (correct response)

Feedback**:** *Posting details about an upcoming deployment on social media is prohibited in accordance with DODI 5400.17.*

Lesson 6 Activities

Responding to Unauthorized Disclosure Activity

You receive an email from a journalist with a national publication, asking you for a comment about the range of a new missile. What should you do with this email?

○ Reply with Comment
○ Reply and CC Security Manager
⊙ Report to Security Manager (correct response)

Feedback**:** *When approached for comment from a journalist, do not make a statement or comment that confirms or denies the accuracy of the information; you should follow your Component guidance and report this request to your Security Manager.*

Reporting Activity

Review the scenario where your coworker approaches with Top Secret documents he found in the bathroom. Knowing the reporting steps, what should you do next?

- ○ Ask them to shred it
- ⦿ Safeguard it and report it to your Security Manager (correct response)
- ○ Tell them to report it
- ○ Safeguard it and tell them not to say anything

Feedback: *When you recognize that CNSI is improperly safeguarded, you must ensure you safeguard it in the appropriate manner and notify your Security Manager or Facility Security Officer (FSO).*