Unauthorized Disclosure of Classified Information and Controlled Unclassified Information

Course Introduction

Introduction

Public service, notably service in the United States Department of Defense or DoD, is a public trust. That trust is bounded by the Oath of Office we took willingly.

To carry out our responsibilities, we are privy to some of the most sensitive and closely held information in our land. It is a violation of our oath to divulge, in any fashion, non-public DoD information, classified or unclassified, to anyone without the required security clearance as well as a specific need to know in performance of their duties. Divulging information in violation of these precepts places our troops, our intelligence operations, and our technological advantages over our foes at risk.

We must be vigilant in executing our responsibility to prevent disclosure of any Information not authorized for release outside of the Department of Defense: All hands must be alert to prevent unauthorized disclosure of non-public information for any reason, whether by implied acknowledgment or intentional release.

We are a Department at war, and the increasingly complex security challenges call for increased vigilance in protecting our secrets. We must always be mindful of the obligations we have to each other and the Nation we have sworn to protect.

Course Learning Objectives

Narrator: Welcome to the Unauthorized Disclosure or UD of Classified Information and Controlled Unclassified Information or CUI Course.

Following course completion, you should be able to describe unauthorized disclosure, demonstrate how to protect classified information and CUI from UD, and apply the steps for reporting a UD.

What Is UD?

Introduction

Learning Objectives

- Identify types of unauthorized disclosure (UD)
- Identify misconceptions about UD
- Distinguish between UD and protected disclosures under the Whistleblower Protection Enhancement Act (WPEA)

Getting Started

Narrator: JB, the security manager, enters the break room to post some material about Unauthorized Disclosure or UD of Classified Narrator: JB, the security manager, enters the break room to post some material about Unauthorized Disclosure or UD of Classified Information and Controlled Unclassified Information or CUI.

JB: Hi, I hope everyone is having a great day. I just posted a document about UD of Classified Information and CUI.

Martin: JB, I know you're busy, but since you're here would you mind giving me a brief overview of this before you go?

JB: Sure. Heather, would you like to listen in?

Heather: No thanks, I'm going to head back to my desk, I'll try to check it out later.

Definition & Policy

JB: Let me first define Unauthorized Disclosure. Unauthorized Disclosure, or UD, is the communication or physical transfer of classified information or controlled unclassified information, or CUI, to an unauthorized recipient. Here is a list of key policies centered around UD.

Key Policies for Unauthorized Disclosure

- Executive Order (E.O.) 13526, Classified National Security Information
- Intelligence Community Directive (ICD) 701, Unauthorized Disclosure of Classified National Security Information
- DoD Directive (DoDD) 5210.50, Management of Serious Security Incidents Involving Classified Information
- DoD Manual (DoDM) 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information
- DoD Instruction 5200.48, Controlled Unclassified Information

CUI is discussed in a separate CDSE product.

Definition & Policy (cont.)

Martin: JB before we continue let me ask, who typically commits UDs?

JB: That's an excellent question. Typically, UDs are committed by an insider, you know, a person who has or had been granted eligibility for access to classified information or eligibility to hold a sensitive position.

Martin: Ok, that's what I was thinking but I wasn't sure.

Types of UD

Narrator: The threat that an insider may do harm to the security of the United States or U.S. requires the integration and synchronization of programs across the Department. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of resources or capabilities (as noted in DoDD 5205.16).

JB: UDs can include damage to the U.S. through the public domain, data spills, espionage, and improper safeguarding of national security information.

More examples of UD types can be found on the course Resources.

Public Domain

JB: The first type of UD is the release of classified information or CUI in the public domain. This information can come in the form of, but is not limited to, podcasts, print articles, internet-based articles, books, journals, speeches, television broadcasts, blogs, and postings. An example is when an individual with access to classified information shares that vital information with a journalist who then releases it.

Data Spills

JB: Data spills are willful, negligent, and inadvertent disclosures of classified information or CUI transferred onto an information system not authorized at the appropriate security level or not having the required CUI protection or access controls. An example of a data spill is when an individual with access to classified information sends a classified email across a network that is not authorized to process classified information.

Espionage

JB: Espionage is activities designed to obtain, deliver, communicate, and/or transmit classified information or CUI intended to aid a foreign power. An example of espionage is when an individual with access to classified information willfully provides this information to a foreign intelligence entity.

Improper Safeguarding of Information

JB: Improper safeguarding of information is defined as using inappropriate measures and controls to protect classified information or CUI. An example of improper safeguarding of information is when an individual with access to classified information accidentally leaves this information in the bathroom and it is found by an uncleared facility custodian.

Types of UD (cont.)

JB: I want to discuss some misconceptions and the Whistleblower Protection Enhancement Act or WPEA. Following, I'll send additional UD information to you via email.

Martin: Okay. Sounds good.

Misconceptions of UD

JB: There are a few misconceptions about UD like classified information or CUI appearing in the public domain, or journalist privilege and some additional misconceptions.

Classified Information or CUI Appearing in the Public Domain

JB: If classified information or CUI have been put in the public domain, then it is okay for employees to freely share it. This is a misconception!

Even though classified information or CUI appear in the public domain, such as in a newspaper or on the internet, it is still classified or designated as CUI until an official declassification decision has been made, or in the case of CUI, it is no longer designated as such.

Journalist Privilege

JB: Cleared employees who disclose classified information or CUI to a reporter or journalist may receive protection through "journalist privilege," which allows reporters and journalists to protect their sources during grand jury proceedings. This is also a misconception!

Employees will not be afforded protection by journalist privilege if they disclose classified information or CUI to a reporter or journalist.

Additional Misconceptions

JB: Manuscripts, books, etc. can be submitted to an editor or publisher before undergoing a security review from the Defense Office of Prepublication and Security Review or DOPSR.

This is incorrect. A security review protects classified information, CUI, and unclassified information that may individually or in compilation lead to the compromise of classified information or disclosure of operations security. I'll talk more about security reviews later.

Once I leave my organization, the Non-Disclosure Agreement or NDA no longer applies.

This is also incorrect. Understand that the NDA we sign is a lifetime agreement with the federal government. I encourage you to review the Termination Briefing Short offered by CDSE.

Misconceptions of UD (cont.)

Martin: JB, I sort of remember some of this being said during my initial security briefing and even during my annual briefing. But to tell you the truth, it's a lot of information to remember.

JB: I realize it's a lot of information, but to carry out our responsibilities, we are privy to some of the most sensitive and closely held information. It's a violation of our oath to divulge, in any fashion, classified information or CUI to anyone without the proper access.

Whistleblower Protection Enhancement Act

Martin: So, JB let me ask a question. Is whistleblowing the same as reporting a UD?

JB: That's an excellent question. It's very important to understand the difference between whistleblowing and reporting UD. Let's talk about whistleblowing.

Whistleblower Protection Enhancement Act (cont.)

JB: Whistleblowing is used to report information an employee reasonably believes provides evidence of a violation of any law, rule, or regulation, gross mismanagement, a gross waste of funds, abuse of authority, or a substantial danger to public health and safety.

JB: The WPEA broadened the scope of the rights and protections for federal employees who "blow the whistle" on such violations. Within the DoD, there are five different statutes that provide whistleblower protections. Additionally, any and all classified, Special Access Program or SAP or Sensitive Compartmented Information or SCI must be reported via specific channels.

Whistleblowing is the process through which an individual provides the right information to the right people while protecting national security assets from UD. If you really want to learn more about whistleblowing and the WPEA, you should reference the DoD Inspector General (IG) website.

DoD Whistleblower Statutes:

- Presidential Policy Directive 19 – Employees in the Intelligence Community or Employees Having Access to Classified Information
- Title 5, U.S.C., Section 2302 – Appropriated Fund Employees
- Title 10, United States Code (U.S.C.), Section 1034 – Military Service Members
- Title 10, U.S.C., Section 1587 – Non-appropriated Fund Instrumentality Employees
- Title 10, U.S.C., Section 2049 – Contractors, Sub-Contractors, Grantees, Sub-Grantees, and Personal Service Contractors

Knowledge Check 1

Narrator: What do you think should be Martin's answers to these questions?

Question 1 of 7 (multiple choice)
When classified information or CUI appear in books, journals, print articles, internet-based articles, etc., this is considered what type of UD?

- Espionage
- Data Spills
- Public Domain
- Improper Safeguarding of Information

Answer: The correct type of UD is "public domain."

Question 2 of 7 (multiple choice)
Which of the following types of UD involve the transfer of classified information or CUI onto an information system not authorized at the appropriate security level or having the required CUI protection?

- Data Spills
- Public Domain
- Improper Safeguarding of Information
- Espionage

Answer: Data spills are the transfer of classified information or CUI onto an information system not authorized at the appropriate security level or having the required CUI protection.

Question 3 of 7 (multiple choice)
Which of the following terms identify activities designed to obtain, deliver, communicate, or transmit classified information or CUI intended to aid a foreign power?

- Data Spills
- Improper Safeguarding of Information
- Espionage
- Public Domain

Answer: Espionage is identified as activities designed to obtain, deliver, communicate, or transmit classified information or CUI intended to aid a foreign power.

Question 4 of 7
Improper safeguarding of information is defined as using inappropriate measures and controls to protect classified information or CUI.

- True
- False

Answer: True: Improper safeguarding of information is defined as using inappropriate measures and controls to protect classified information or CUI.

Question 5 of 7
Classified information or CUI that has been put in the public domain is free to share.

- True
- False

Answer: False: Classified information or CUI that has been put in the public domain is not free to share.

Question 6 of 7
The policy for the Whistleblower Protection Enhancement Act (WPEA) is the same as that of Unauthorized Disclosure (UD).

- True
- False

Answer: False: There are five DoD Whistleblower statutes: Title 10 USC Sections 1034, 1587, and 2049; Title 5 USC Section 2302; and PPD 19 and the policy for UD is DoDD 5210.50.

Question 7 of 7 (multiple choice)
Whistleblowing should be used to report which of the following?

- Gross mismanagement
- Gross waste of funds
- Substantial danger to public health and safety
- Information disclosed to a reporter or journalist

Answer: Whistleblowing should be used to report gross mismanagement, gross waste of funds, and substantial danger to public health and safety.

Summary

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

- Identify types of unauthorized disclosure
- Identify misconceptions about unauthorized disclosure
- Distinguish between unauthorized disclosure and protected disclosures under the Whistleblower Protection Enhancement Act (WPEA)

Protecting Classified Information and Controlled Unclassified Information (CUI) from UD

Introduction

Lesson 2: Protecting Classified Information and Controlled Unclassified Information (CUI) from UD

Learning Objectives

- Recognize access, safeguarding, marking, storage, and classification requirements for classified information
- Interpret prepublication review requirements
- Recognize the role of the Public Affairs Office (PAO)
- Recognize DoD policy and authorized use of social media

Requirements for Access and Safeguarding and Storage

Narrator: As promised, Martin just received an email from JB with additional information about UD.

Subject – Unauthorized Disclosure: Protecting Classified Information and CUI

From – Jackie Brown

Martin, it was great speaking with you today. As promised, below is more information about UD.

Protecting Classified Information and CUI from UD:

- Requirements for Access
- Safeguarding and Storage

After you finish reviewing these items, take some time and access the intranet for information covering marking and classification types.

Afterwards, come to my office and we can discuss further.

Thanks,

Jackie Brown "JB"
Security Manager

Requirements for Access

Narrator: Authorized recipients must meet certain requirements for access to classified information and CUI.

They must have a favorable determination of eligibility at the proper level, have a "need-to-know", and have signed an appropriate NDA before accessing classified information.

Any individual who fails to meet these requirements is not authorized to access classified information.

Authorized holders must also meet certain requirements to access CUI in accordance with a lawful government purpose which may include activity, mission, function, operation, and endeavor that the U.S Government authorizes or recognizes as within the scope of its legal authorities.

For more info, refer to: 32 CFR Part 2002 in the course Resources.

Safeguarding and Storage

Narrator: E.O. 13526, DoDM 5200.01, and the National Industrial Security Program Operating Manual, or NISPOM, provide guidance for safeguarding classified information from UD. It is your responsibility to follow this guidance.

You must properly handle classified information, including the use of classified document cover sheets when classified information is outside of a General Service Administration or GSA approved security containers.

Stored classified information in GSA-approved security containers or other approved methods when the information is not under personal observation and control, follow guidelines for the reproduction of classified information, which include using only copiers and printers designated specifically for reproducing classified information.

Follow appropriate procedures for transmission and transportation of classified information, and follow appropriate guidelines when destroying or disposing of classified information.

Safeguarding and Storage (con't.)

Narrator: CUI must always be safeguarded in a manner that minimizes the risk of UD while allowing timely access by authorized holders. For more information, reference the CUI Toolkit in the course Resources. You are required to protect classified information throughout your life, even when you are no longer affiliated with the federal government and/or the military.

Reference DoDM 5200.01, Volume 3, Enclosure 2 and Enclosure 3 in the course Resources.

Marking

Narrator: Following JB's suggestion, Martin conducts a search on the intranet for information on markings and classification types.

Martin's Desktop Intranet

Intranet – Unauthorized Disclosure
- Marking
- Classification Types

Marking

Narrator: All classified information shall be clearly identified by authorized security classification and control markings; authorized abbreviations and portion markings.

Markings must be conspicuous, immediately apparent, and alert holders to the presence of classified information, identify, as specifically as possible.

The exact information needing protection and the level of protection required, give information on the sources and reasons for classification of the information, identify the office of origin and document originator.

Applying the classification markings, provide guidance on information sharing, and warn holders of special access, dissemination control, and safeguarding requirements, and provide guidance on downgrading and declassification of classified information.

More information can be found in DoDM 5200.01, Volume 2 in the course Resources.

Classification Types

Narrator: There are two types of classification; original and derivative.

Original classification
Original classification is the initial determination that information needs protection because its disclosure could be reasonably expected to cause identifiable or describable damage to national security.

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

More Information:
See DoDM 5200.01, Volume 3 and DoDM 5200.45 available in the course Resources.

Prepublication Review

JB: Hi, Martin. Good to see you again. How is everything going with UD?

Martin: Pretty good. Although, I do have a question.

JB: Let's hear it.

Martin: I heard one of our former colleagues is writing a memoir including some information about their work here. How does that comply with UD regulations?

JB: Great question. If they choose to publish, there are some requirements they need to be aware of. I have prepublication review information on my computer. You can follow along using the hard copy as we go through the requirements.

Prepublication Review (con't.)

JB: If you or anyone has ever had access to classified information and/or CUI, you may be in a position to write books, articles, speeches, briefings, etc.

However, if these writings contain DoD information, there are certain rules you must follow before those items may be publicly released. Public release includes, but is not limited to, sending any book, manuscript, or article to a publisher, editor, movie producer, or game purveyor, and distributing any speech, briefing, article, or content that will be publicly available. As outlined in DoD Instruction, or DoDI, 5230.09, Clearance of DoD Information for Public Release, you must submit the materials to the DOPSR for a prepublication review.

JB: Prepublication review is the process by which information proposed for public release is examined by the DOPSR for compliance with established national and DoD policies and 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 disclosure of operations security.

Martin: I vaguely remember this being part of my initial security briefing. Let me ask you this…What about resumes? Are they also sent to DOPSR? As military members and federal civilian employees, we often work in special programs and we may mention unclassified information on our resume.

JB: Martin, that's an excellent question. Although not in policy, it's a best practice to ensure you're current or last command conduct a security review of your resume and cover letter. Resumes and cover letters are not sent to DOPSR for review.

Martin: Well, what's the Public Affairs Office or PAO role in all this?

JB: Martin you are asking some great questions. The PAO is distinctly different from DOPSR. Let's take a look at their role.

Who has to submit for prepublication review?
Past and present:

- Government civilian employees
- Contractor personnel
- Military personnel
- Retirees

DOPSR Prepublication Brochure
Refer to the DOPSR Prepublication Brochure for:

- What to submit
- Where to submit
- Submission timelines

Note: It is a best practice to ensure your current/previous command conduct a security review of your resume and cover letter prior to your releasing it to the public. Resumes and cover letters are not sent to DOPSR for review.

Public Affairs Office (PAO)

JB: Although the PAO, does not review material for classified information or CUI, they do play a role in the process of information that is released to the public. The PAO conducts a review for specific considerations like, political views, things that bring discredit to the military or federal government, or are otherwise offensive.

With that in mind, the following sequential steps are used to incorporate the PAO into a process for releasing information to the public:

1. Security review, to be conducted by local/command security manager and then the DOPSR.
2. The PAO conducts a review for public affairs-specific considerations.
3. Following approval, information may be released to the public, via appropriate channels.

JB: The last item to review is social media guidance.

Social Media Guidance

JB: You must always be mindful of your obligation to protect classified information and CUI to prevent its unauthorized disclosure.

DoDM 5200.01, Volume 3 states that when using social networking services, such as Facebook, Twitter, YouTube, LinkedIn, wikis, Instagram, and blogs, the requirements for protecting classified information and CUI from UD, and the penalties for ignoring those requirements, are the same as when using other media and methods of dissemination.

JB: On a side note, many years ago there was a military secrecy campaign that stated: What you see here, what you hear here, what you do here, when you leave here, it stays here.

Martin: Hmm, that's interesting. Perhaps, we should resurrect that campaign?

More Information:
Do's and Don'ts can be found on the course Resources.

Knowledge Check 2

Narrator: Before moving on, complete these knowledge checks.

Question 1 of 6 (multiple answer)
You have a classified document you would like to share with your coworker, Julie. What requirements must Julie meet to be an authorized recipient?

- Need-to-know
- The same rank or position you hold or higher
- Signed NDA
- Favorable eligibility determination for access to the level of the classified information to be shared

Answer: Julie must have a need-to-know, a signed NDA, and a favorable eligibility determination for access to the level of the classified information to be shared.

Question 2 of 6 (multiple answer)
Which of the following describes your responsibility to protect classified information from unauthorized disclosure?

- Take it home to analyze the information first
- Use classified document cover sheets
- Follow guidelines for the reproduction of classified information
- Store classified information in
- GSA-approved security containers or other approved methods

Answer: You must use classified document cover sheets, follow guidelines for the reproduction of classified information, and store classified information in GSA-approved security containers or other approved methods.

Question 3 of 6 (fill in the blanks)
Fill in the blanks using one of the answer options below.

_____ is the initial determination that information needs protection, while _____ is the process of using existing classified information to create new material and marking that newly developed material consistent with classification markings.

- Derivative Classification, Original Classification
- Tough Classification, Simple Classification
- Original Classification, Derivative Classification
- New Classification, Old Classification

Answer: Original classification is the initial determination that information needs protection, while derivative classification is the process of using existing classified information to create new material and marking that newly developed material consistent with the classification marking.

Question 4 of 6 (multiple choice)
As an individual with access to classified information and CUI, you may write books, articles, speeches, and briefings. If they contain official DoD information, those items must go through which of the following?

- Examination
- Marking Review
- Portion Review
- Security Review

Answer: If a book, article, speech or briefing contains official DoD information, it must go through a security review.

Question 5 of 6
The PAO reviews content for classified information and CUI.

- True
- False

Answer: False: The PAO does not review content for classified information and CUI.

Question 6 of 6
You may disclose classified information when using social media outlets.

- True
- False

Answer: You may not disclose classified information when using social media outlets.

Summary

JB: Martin, thanks for spending time with me to discuss protecting classified information and CUI. I hope you found the information helpful.

You should be able to address these items.

Keep in mind that the message on the back of the binder is something that people working with sensitive information should live by. What you see here, what you hear here, what you do here, when you leave here, it stays here.

- Recognize access, safeguarding, marking, storage, and classification requirements for classified information
- Interpret prepublication review requirements
- Recognize the role of the Public Affairs Office (PAO)
- Recognize DoD policy and authorized use of social media

UD Reporting

Introduction to UD Reporting

Learning Objectives

- Explain how to respond to information appearing in the public domain
- Sequence the steps for reporting unauthorized disclosures

Introduction to UD Reporting (con't.)

Martin: JB, this has been great.

JB: Let's break for lunch and when we come back, we can talk about UD reporting.

Narrator: As Martin goes next door to grab a salad, he sees his colleague, Heather, sitting a few tables away and talking with Angela, a local reporter from Channel news.

He can see that they are conducting an interview in which notes are being taken and a voice recorder is being used.

However, Martin isn't alarmed, until he hears a classified project mentioned. That's when he listens closer.

Angela: Again, I want to thank you for your time today. To wrap up this report, I just have one last question.

Heather: Okay.

Angela: Has your department had issues developing the new Wing Model Five Missile?

Heather: I'm sorry, I can't provide any additional information.

Information Appearing in the Public Domain

Narrator: After overhearing one of his colleagues discuss a classified project with a reporter, Martin immediately goes to JB's office to discuss what he witnessed.

JB: Hi, Martin. Are you ready to get started?

Martin: Before we get started, I want to discuss something I overheard on my lunch break.

JB: Okay, I'm listening.

Martin: Well, having learned so much about UD, I think I may have witnessed Heather giving classified information to a reporter.

She didn't go into much detail about our classified project, but when asked "Has your department had any issues developing the new Wing Model Five Missile?" she responded with, "I'm sorry, I can't provide any additional information."

I'm not sure if what she said is a violation of any kind, so I wanted to run this information by you.

JB: Well Martin, I'm glad you recognized the need to bring this to my attention, as I am the security manager.

JB: Information which could appear in the public media is a serious matter and should be properly addressed anytime it occurs. This includes being approached or contacted by a representative of the media.

JB: If this happens to you, do not make any statement or comment that confirms or denies accuracy of the information requiring protection. Instead, report it directly to your security manager like you did.

Martin: I understand. So, if Heather had replied "no comment" or something similar then she would have not committed a UD incident?

JB: Exactly. Let me explain the steps for reporting a UD incident.

For more information, refer to: DoDM 5200.01, Vol 3, and DoDI 5200.48, Section 3.9 in the course Resources.

Steps to Reporting a UD Incident

JB: For the purpose of our discussion I organized the reporting into eight digestible steps.

Steps to Reporting a UD Incident

Step 1 - Safeguard

Step 2 - Report

Step 3 – Inquire

Step 4 - Investigate

Step 5 – Evaluate

Step 6 – Elevate

Step 7 - Correct

Step 8 - Sanction

Step 1: Safeguarding

JB: The first step is safeguarding. Safeguarding is when classified information is secured by placing it into a GSA-approved security container or other approved methods. CUI must also be safeguarded in a manner that minimizes the risk of UD.

Step 2: Reporting

JB: Step two is reporting the information to your security manager or FSO. The first two steps are essential and the responsibility of anyone who believes they have witnessed, have discovered, or have knowledge of a UD.

Before moving on, it is important to note that steps three through seven are the responsibility of the security manager or FSO.

Narrator: Steps one through two applies to everyone, however, if you are a security manager or FSO please reference the downloadable job aid on the course Resource page to see which steps applies directly to your personnel.

JB: When classified information is involved, a report is always made to the Original Classification Authority, or OCA, who will conduct a damage assessment. The report to the OCA may vary depending on whether you are a security manager or FSO. Certain types of classified information or specific circumstances require unique handling or consideration of additional reporting requirements.

For further clarification, see the student job aid on course Resources.

Step 8: Sanction

JB: Finally, step eight is where sanctions are handed down. Criminal, civil, and/or administrative sanctions may be brought against an individual who fails to protect classified information and CUI from UD. As a reminder, this step applies to everyone along with step one and two.

More information: According to DoDD 5210.50 “Management of Serious Security Incidents Involving Classified Information”:

- Training on the prevention, identification, and reporting of serious security incidents will be provided to all DoD personnel authorized access to classified information. For more information on sanctions involving CUI, please refer to DoDI 5200.48 Controlled Unclassified Information.

- The prevention of serious security incidents is a responsibility shared by all DoD personnel.

For further clarification, see the job aid on course Resources.

Knowledge Check 3

Narrator: Let's see how well you can answer the following questions.

Question 1 of 3 (multiple choice)
What is the first step in reporting an incident of Unauthorized Disclosure?

- Place items in an opaque zip lock bag
- Place items in a GSA-approved security container or other approved method
- Place items in a manila folder
- Hand items to your security manager as quickly as possible

Answer: The first step in reporting an incident of Unauthorized Disclosure is to place items in a GSA-approved security container or other approved method.

Question 2 of 3 (multiple choice)
After completing step one of reporting an Unauthorized Disclosure incident, what is your next step?

- Conduct inquiry field experiment
- Report to your security manager or FSO
- Call the Federal Bureau of Investigation
- Tell your co-worker

Answer: Step two of reporting is to report the incident to your security manager or FSO.

Question 3 of 3 (multiple answer)
What must you do if approached or contacted by a representative of the media seeking a response to information appearing in the public domain?

- Report it to your security manager or FSO
- Make a statement
- Neither confirm nor deny the information in question
- Always tell the truth

Answer: Do not make any statements or comments that confirm or deny the information in question and report it to your security manager or FSO.

Summary

JB: I'm glad I could bring everything full circle for you. You did the right thing and we all appreciate it.

By now, you should know how to respond to information appearing in the public domain, and the steps for reporting UD.

Martin: Thank you so much for getting me up to speed on UD.

JB: No problem, and always remember: What you see here, what you hear here, what you do here, when you leave here, it stays here.

Congratulations!

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

You should now be able to describe unauthorized disclosure, demonstrate how to protect classified information and CUI from UD, and apply the steps for reporting a UD.