Student Guide

Unauthorized Disclosure Refresher

Lesson 1: Course Introduction

Contents

Overview

Definitions

Welcome to the Unauthorized Disclosure Refresher course! In this course, you will review your understanding of unauthorized disclosure by completing a series of scenarios that all take place in a typical office.

Unauthorized disclosure is the communication or physical transfer of classified information or controlled unclassified information (CUI) to an unauthorized recipient. These disclosures can be intentional or inadvertent, but either way, they can have serious repercussions.

For example, media disclosure of classified information has significantly impaired U.S. capabilities against our hardest targets and done grave harm to national security.

In this course, you will review the types of unauthorized disclosure and the impacts of such disclosures. You will also review how to protect information, and the actions to take if you learn of suspected or actual incidents of unauthorized disclosure.

Course Overview

To successfully complete this course, you will need to demonstrate your ability to carry out the activities listed in the course objectives. Please take a moment to review them.

- Identify the types of unauthorized disclosure
- Recognize the impacts of unauthorized disclosure
- Demonstrate how to protect classified information and controlled unclassified information (CUI) to prevent unauthorized disclosure
- Determine actions to take if you learn of suspected or actual unauthorized disclosure

Introduction to Your Role

In this course, you will review your understanding of unauthorized disclosure by taking on the role of an employee with a responsibility to protect classified information and CUI.

As you complete the activities, you may wish to review a particular topic area. Basic review material for each activity will be available for review via the hints boxes.

Student Guide

Unauthorized Disclosure Refresher

Lesson 2: What is Unauthorized Disclosure?

Contents

Types of Unauthorized Disclosure

E-mail Notification: Training Video 1

You just received an e-mail. It looks like it's from Alison Green, your supervisor.

To: The team
From: Alison Green
Subject: Training Video: Types of Unauthorized Disclosure
Attachment: TypesofUD.mp4

Hello Team,
Take a look at this training video! It provides a good short summary of the types of unauthorized disclosure that you should be aware of.
Thanks,
Alison

It looks like your supervisor sent you a training video on Types of Unauthorized Disclosure.

Training Video Narrator

You know you need to prevent unauthorized disclosure – but did you know that there are different types of unauthorized disclosure?

If classified information or controlled unclassified information – called CUI – is deliberately disclosed to the media, it is considered a leak.

Activities that are designed to obtain or transmit classified information or CUI in order to harm the United States or provide advantage to a foreign nation or transnational entity are considered espionage.

Finally, the willful, negligent, or even inadvertent disclosure of classified information or CUI across computer systems is considered a spill.

The most common spills occur over the internet, through compilation of unclassified data elements, or via e-mail – either in the body of a message or in an attachment. Spills are very serious, especially when classified information is involved, and can create the potential for rapid and widespread unauthorized disclosure. In fact, classified spills are so serious that the term – Negligent Discharge of Classified Information, or NDCI – has been coined to connote its seriousness.

Do you know what you need to do to prevent all of these types of unauthorized disclosure?

Misconceptions

E-mail Notification: Help a Coworker

You just received another e-mail from Alison Green.

To: You
From: Alison Green
Subject: Help for Jonathan

Hi there,

I know you're busy, but I think our new employee, Jonathan Kilsythe, may have some misconceptions about what constitutes an unauthorized disclosure. Unfortunately, I'll be in meetings all day long and won't have time to work with him.

Could you please give him a call (x4312) and answer any questions he has?

Thanks,
Alison

It looks like your supervisor needs you to help get your coworker Jonathan up to speed. You give Jonathan a call.

Call with Jonathan: Misconceptions

Jonathan: Hi, this is Jonathan! I'm so glad you called – I was just talking to Alison and I realized some of what I thought I knew about unauthorized disclosure may be wrong!

If you need help with the following series of questions, refer to the Hints table below.

Misconceptions Regarding Unauthorized Disclosure - Hints

- If classified information appears in the news media, the internet, or other outlets in the public domain, the information is still considered classified until it is officially declassified:
  - Cleared employees are still legally bound not to view it
  - Cleared personnel can be subject to sanctions if they seek out classified information in the public domain, acknowledge its accuracy or existence, or proliferate the information in any way
  - If cleared employees do view it, then it must be reported as a data spill and the spill must be isolated and contained on the computer or other information system used to view it (e.g. BlackBerry, smartphone, tablet, etc.)
- "Journalists' Privilege" does not allow reporters to protect their sources during grand jury proceedings
- The Whistleblower Protection Act (PPD-19):
  - Protects employees from direct retaliation for acts of reporting protected disclosures
  - Does not protect employees who unlawfully disclose classified information
- The First Amendment does not guarantee protection to a cleared employee who discloses classified information unlawfully
- Cleared employees are responsible for the protection of classified information or CUI, even after they are no longer employed by the government or by a cleared government contractor

Misconceptions: Question 1

Jonathan: For example, once information is out there on the internet it's no longer classified, right?

Jonathan believes that once classified information enters the public domain it is no longer considered classified.

Decide whether Jonathan is right or wrong.

- ○ Right. As soon as information enters the public domain it is considered declassified.
- ○ Wrong. Even after classified information enters the public domain, it is still considered classified until it is officially declassified.

Do not proceed to the next page until you select your response.

Misconceptions: Question 1 Answer

Correct Response: Jonathan is wrong. If classified information appears in the public domain, the information is still considered classified until it is officially declassified. Therefore, it would be considered an unauthorized disclosure.

Misconceptions: Question 2

Jonathan: Huh. I didn't know that. Still, it would be okay for me to view the information, because I have a clearance, right?

Jonathan believes that, because he has a clearance, he is permitted to view classified information that has been leaked to the public domain.

Decide whether Jonathan is right or wrong.

- ○ Right. Because Jonathan has a clearance he may view information leaked to the public domain.
- ○ Wrong. Cleared employees may not view classified information leaked to the public domain.

Do not proceed to the next page until you select your response.

Misconceptions: Question 2 Answer

Correct Response: Jonathan is wrong. Cleared employees are legally bound not to view classified information leaked to the public domain, and can be subject to sanctions if they seek it out, acknowledge its accuracy or existence, or proliferate the information in any way.

Misconceptions: Question 3

Jonathan: Interesting! I know there have been some high profile cases like this lately, and I've heard a lot about the "Whistleblower Protection Act." What does that do?

Jonathan has asked about the Whistleblower Protection Act (PPD-19). What protections does this act grant employees?

Answer Jonathan's question by selecting all that apply.

- ☐ Protects employees from direct retaliation for reporting waste, fraud, abuse, and other protected disclosures
- ☐ Protects employees from prosecution for the unlawful disclosure of classified information if it was done in the public's interest

Do not proceed to the next page until you select your response.

Misconceptions: Question 3 Answer

Correct Response: The Whistleblower Protection Act protects employees from direct retaliation for reporting waste, fraud, abuse, and other protected disclosures. It does NOT protect employees who unlawfully disclosure classified information for any reason.

Misconceptions: Question 4

Jonathan: You know, I don't plan to stay at this job forever. How long will I be responsible for protecting against unauthorized disclosure?

Jonathan would like to know how long he will be responsible for the protection of classified information and CUI.

Decide how you want to respond to Jonathan.

- ○ Until he leaves his current position
- ○ For the rest of his career, until he retires
- ○ Until his security clearance expires
- ○ He is required to protect them even after he retires or leaves employment

Do not proceed to the next page until you select your response.

Misconceptions: Question 4 Answer

Correct Response: Jonathan is responsible for the protection of classified information and CUI even after he retires or leaves employment.

Impacts

Call with Jonathan: Impacts

Jonathan: Thanks! I think you've cleared up my misunderstandings.

But I have some questions about the impact of unauthorized disclosure as well, if you don't mind answering a few more of my questions…

If you need help with the following series of questions, refer to the Hints table below.

Impacts of Unauthorized Disclosure - Hints

- Examples of damage caused by unauthorized disclosure
  - Damage to national security
  - Undermines ongoing and planned U.S. operations
  - Potential loss of life
  - Damage to intelligence community sources and methods
  - Effect on international alliances
  - Financial costs
  - Reduces technological advantage over adversaries
  - Impact to foreign policy
  - Undermine the public's confidence and trust
  - Benefits adversaries wishing to harm U.S.
- Sanctions that may be applied if employees are responsible for unauthorized disclosure of classified information or CUI include:
  - Uniform Code of Military Justice (UCMJ):
    - Loss of rank
    - Loss of pay
    - Dishonorable discharge
    - Incarceration
  - Civil litigation:
    - Loss of payments or royalties
  - Administrative sanctions:
    - Suspension without pay
    - Revocation of security clearance
    - Termination of employment
    - Loss of DoD contracts post-employment
  - Criminal sanctions:

- Incarceration
- Fines

o Loss of federal retirement benefits

Impacts: Question 1

Jonathan: I guess I'm just wondering – what's the big deal? What could happen if information gets out?

Jonathan has asked about the impact of unauthorized disclosure. Which of the following are examples of damage caused by unauthorized disclosure?

Answer Jonathan's question by selecting all that apply.

- ☐ Undermines ongoing and planned U.S. operations
- ☐ Damages intelligence community sources and methods
- ☐ Incurs financial costs
- ☐ Impacts foreign policy
- ☐ Undermines the public's confidence and trust
- ☐ Benefits adversaries wishing to harm U.S.
- ☐ Reduces technological advantage over adversaries
- ☐ Puts lives at risk

Do not proceed to the next page until you select your response.

Impacts: Question 1 Answer

Correct Response: All of these – and more – are examples of damage that could be caused by unauthorized disclosure.

Impacts: Question 2

Jonathan: That's pretty serious! I assume there are significant consequences for those responsible?

Jonathan has asked about the consequences for those responsible for unauthorized disclosure. Which of the following are examples of sanctions that may be imposed?

Answer Jonathan's question by selecting all that apply.

- ☐ Loss of rank
- ☐ Fines
- ☐ Revocation of security clearance
- ☐ Suspension without pay
- ☐ Termination of employment
- ☐ Incarceration

Do not proceed to the next page until you select your response.

Impacts: Question 2 Answer

Correct Response: These are ALL just some of the military, civil, administrative, and criminal sanctions that may be imposed on individuals responsible for unauthorized disclosure. This applies to both the unauthorized disclosure of classified information and CUI.

How Did You Do?

Consider how you did on the questions in this lesson. If you need to review any of the information in more detail, refer to the appropriate Job Aid included below and on the following page.

Misconceptions Regarding Unauthorized Disclosure Job Aid

Misconceptions Regarding Unauthorized Disclosure

- If classified information appears in the news media, the internet, or other outlets in the public domain, the information is still considered classified until it is officially declassified:
  - Cleared employees are still legally bound not to view it
  - Cleared personnel can be subject to sanctions if they seek out classified information in the public domain, acknowledge its accuracy or existence, or proliferate the information in any way
  - If cleared employees do view it, then it must be reported as a data spill and the spill must be isolated and contained on the computer or other information system used to view it (e.g. BlackBerry, smartphone, tablet, etc.)
- "Journalists' Privilege" does not allow reporters to protect their sources during grand jury proceedings
- The Whistleblower Protection Act (PPD-19):
  - Protects employees from direct retaliation for acts of reporting protected disclosures
  - Does not protect employees who unlawfully disclose classified information
- The First Amendment does not guarantee protection to a cleared employee who discloses classified information unlawfully
- Cleared employees are responsible for the protection of classified information or CUI, even after they are no longer employed by the government or by a cleared government contractor

Impacts of Unauthorized Disclosure Job Aid

Impacts of Unauthorized Disclosure

- Examples of damage caused by unauthorized disclosure
  - Damage to national security
  - Undermines ongoing and planned U.S. operations
  - Potential loss of life
  - Damage to intelligence community sources and methods
  - Effect on international alliances
  - Financial costs
  - Reduces technological advantage over adversaries
  - Impact to foreign policy
  - Undermine the public's confidence and trust
  - Benefits adversaries wishing to harm U.S.
- Sanctions that may be applied if employees are responsible for unauthorized disclosure of classified information or CUI include:
  - Uniform Code of Military Justice (UCMJ):
    - Loss of rank
    - Loss of pay
    - Dishonorable discharge
    - Incarceration
  - Civil litigation:
    - Loss of payments or royalties
  - Administrative sanctions:
    - Suspension without pay
    - Revocation of security clearance
    - Termination of employment
    - Loss of DoD contracts post-employment
  - Criminal sanctions:
    - Incarceration
    - Fines
  - Loss of federal retirement benefits

Student Guide

Unauthorized Disclosure Refresher

Lesson 3: Safeguarding Classified Information and CUI

Contents

Safeguarding Procedures

E-mail Notification: Training Videos 2 and 3

You just received another e-mail from Alison Green.

To: The team
From: Alison Green
Subject: Two More Training Videos
Attachment(s): Safeguarding Procedures; Classification and Declassification

Hello Team,

I've found two more great training videos for you. One is about safeguarding classified information, and the other is about classification and declassification procedures. Please take a look – it will only take a few minutes of your time.

Thanks,
Alison

It looks like Alison sent you more training videos.

Safeguarding Procedures

Training Video Narrator

If you have been granted access to classified national security information, or NSI, then you probably already know how important it is for you to safeguard that information; doing so protects our soldiers in the field and our security at home.

In order to safeguard NSI, you MUST follow all rules for storage, handling, reproduction, transmission and transportation, information system use, and destruction. DoD employees can find the requirements for these procedures in DoDM 5200.01, Vol. 1-3, DoD Information Security Program. Cleared contractors should reference DoD 5220.22-M, the National Industrial Security Program Operating Manual, or NISPOM.

Controlled unclassified information, or CUI, is also subject to safeguarding requirements and access restrictions – for details, DoD employees should see DoDM 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information. Contractors and subcontractors can find specific requirements for safeguarding CUI included in contract documents, such as the statement of work, contract clause(s), or DD Form 254, the DoD Contract Security Classification Specification.

Remember, when using social networking services, the requirements for protecting

classified information from unauthorized disclosure – and the penalties for failing to do so – are the same as when using other media and methods of dissemination.

Finally, remember, now that you have been granted access, you have a responsibility to protect NSI throughout your life, even after you are no longer a government employee, or working for a cleared government contractor.

Do you know what you need to do to prevent all of these types of unauthorized disclosure?

Classification and Declassification

Training Video Narrator

To properly protect classified national security information, or NSI, you must first understand and apply appropriate procedures for classification and declassification.

The decision to initially classify national security information is a government responsibility and is carried out by Original Classification Authorities, or OCAs. To make this decision, OCAs determine the level of damage that would occur in the event of an unauthorized disclosure.

Derivative classifiers carry these markings forward, and must ensure proper classification markings appear on all classified information.

You must also understand and apply the policies and procedures for downgrading and declassifying NSI so that, if applicable, it is downgraded to the appropriate level at the appropriate time, and that it is declassified at a specific date or following a specific event.

To learn more about original classification, derivative classification, and marking classified information, see the Original Classification Authority, Derivative Classification, and Marking Classified Information courses, available through CDSE's Security, Training, Education and Professionalization Portal, or STEPP.

Disclosure Authorization

Call with Cathy: Disclosure Authorization

You just received a phone call from a coworker.

Cathy: Hi, this is your coworker, Cathy! I was wondering if we could talk about Project W – I heard you are doing some interesting things!

If you need help with the following series of questions, refer to the Hints table below.

Authorized Recipients of Classified Information and CUI – Hints

- Authorized recipients of classified information have:
  - Favorable determinations of eligibility for access to classified information at the proper level
  - "Need-to-know" for the classified information
  - Signed SF-312, Classified Information Nondisclosure Agreement (NDA)
- Authorized recipients of CUI have:
  - "Need-to-know" for access to CUI
  - Complied with other additional limitations and regulations as applicable
- Anyone who does not meet the above criteria is UNAUTHORIZED. This may include:
  - Media outlets
  - The general public
  - Coworkers and supervisors
  - Foreign intelligence entities

Disclosure Authorization: Question 1

Your coworker, Cathy, has a SECRET clearance. She wants to discuss a project with CONFIDENTIAL information, but she is not assigned to the project.

Determine whether Cathy is an authorized recipient of this information.

- ○ Yes. Because Cathy's clearance exceeds that of the information, you may discuss the project with her.
- ○ No. Cathy's clearance is not the same as the information, so you may not discuss it with her.
- ○ No. Cathy has an appropriate clearance, but she does not have an appropriate need-to-know.

Do not proceed to the next page until you select your response.

Disclosure Authorization: Question 1 Answer

Correct Response: You should NOT discuss the information with Cathy. She has an appropriate clearance, but she does not have a need-to-know.

Disclosure Authorization: Question 2

Cathy: Oh, I'm sorry – I didn't realize that project was classified! Now that you mention it, I'm scheduled to speak as a subject matter expert at a major public conference next month and some of the programs I work on involve classified information. Can you remind me – who can I discuss classified information with?

Cathy needs to be able to identify authorized recipients of classified information. Authorized recipients MUST have which of the following?

Answer Cathy's question by selecting all that apply.

- ☐ A favorable determination of eligibility for access to classified information at the proper level
- ☐ A position of authority within Cathy's agency
- ☐ A "need-to-know" for the classified information
- ☐ A signed SF-312, Classified Information Nondisclosure Agreement (NDA)

Do not proceed to the next page until you select your response.

Disclosure Authorization: Question 2 Answer

Correct Response: Authorized recipients of classified information have:

- A favorable determination of eligibility for access to classified information at the proper level
- A "need-to-know" for the classified information
- A signed SF-312, Classified Information Nondisclosure Agreement (NDA)

Anyone who has NOT met ALL these criteria is UNAUTHORIZED. Unauthorized individuals may include the media, the general public, foreign intelligence entities, and even coworkers or supervisors.

Prepublication Review

Call with Cathy: Prepublication Review

Cathy: Thanks! So… since I'm presenting a paper at this upcoming conference, is there anything I need to do?

If you need help with the following series of questions, refer to the Hints table below.

Prepublication Review – Hints

- Within the DoD, all material undergoes prepublication review by the Defense Office of Prepublication and Security Review (DOPSR) to ensure it contains no classified information or CUI
- Industry employees must consult their Facility Security Officer (FSO) and Government Contracting Activity (GCA) for guidance
- Prepublication reviews are required before:
  - Sending any book, manuscript, or article to a publisher, editor, movie producer, game purveyor, or their respective support staffs
  - Distributing any speech, briefing, article, or any content that will be publically available
  - Releasing information to the public, even through Congress or the courts
- Per DoDI 5230.29:
  - Prepublication review is NOT a declassification action
  - Anyone submitting material for prepublication review must believe it is unclassified prior to submission
  - Material submitted to DOPSR must first be coordinated and reviewed within the originating DoD Component

Prepublication Review: Question 1

As a DoD employee who works on a project containing classified information, is there anything Cathy needs to do before speaking at the upcoming public conference?

Decide how you want to answer Cathy's question.

- ○ Yes. Cathy should submit her paper for a prepublication review before speaking at the conference.
- ○ No. As long as Cathy ensures no classified material is included in her paper, she does not need to do anything else.

Do not proceed to the next page until you select your response.

Prepublication Review: Question 1 Answer

Correct Response: Cathy should submit her paper for a prepublication review before presenting it at the conference.

Prepublication Review: Question 2

Cathy: So I can submit my paper for prepublication review, and the review will ensure that any classified details I've included are declassified, right?

May Cathy include classified information in the paper she submits for prepublication review?

Decide how you want to answer Cathy's question.

- ○ Yes. Any classified information in Cathy's paper will be either redacted or declassified during prepublication review.
- ○ No. Cathy must believe her paper is unclassified prior to submission for prepublication review.

Do not proceed to the next page until you select your response.

Prepublication Review: Question 2 Answer

Correct Response: Cathy must believe her paper is unclassified prior to submission for prepublication review. Prepublication review is NOT a declassification action!

Prepublication Review: Question 3

Cathy: Ah, okay, good to know. Out of curiosity, do you know of other times prepublication review is required?

Cathy would like to know when prepublication review is required. Which of the following events require prepublication review?

Answer Cathy's question by selecting all that apply.

- ☐ Sending a book, manuscript, or article to a publisher, editor, or producer
- ☐ Distributing a speech, briefing, or article in a public setting
- ☐ Presenting a memo at a closed meeting within your agency
- ☐ Releasing information to the public through Congress or the courts

Do not proceed to the next page until you select your response.

Prepublication Review: Question 3 Answer

Correct Response: The following are examples of events that require prepublication review:

- Sending a book, manuscript, or article to a publisher, editor, or producer
- Distributing a speech, briefing, or article in a public setting
- Releasing information to the public through Congress or the courts

How Did You Do?

Consider how you did on the questions in this lesson. If you need to review any of the information in more detail, refer to the appropriate Job Aid included below and on the following page.

Authorized Recipients of Classified Information and CUI – Job Aid

Authorized Recipients of Classified Information and CUI – Hints

- Authorized recipients of classified information have:
  - Favorable determinations of eligibility for access to classified information at the proper level
  - "Need-to-know" for the classified information
  - Signed SF-312, Classified Information Nondisclosure Agreement (NDA)
- Authorized recipients of CUI have:
  - "Need-to-know" for access to CUI
  - Complied with other additional limitations and regulations as applicable
- Anyone who does not meet the above criteria is UNAUTHORIZED. This may include:
  - Media outlets
  - The general public
  - Coworkers and supervisors
  - Foreign intelligence entities

Prepublication Review – Job Aid

Prepublication Review – Hints

- Within the DoD, all material undergoes prepublication review by the Defense Office of Prepublication and Security Review (DOPSR) to ensure it contains no classified information or CUI
- Industry employees must consult their Facility Security Officer (FSO) and Government Contracting Activity (GCA) for guidance
- Prepublication reviews are required before:
  - Sending any book, manuscript, or article to a publisher, editor, movie producer, game purveyor, or their respective support staffs
  - Distributing any speech, briefing, article, or any content that will be publically available
  - Releasing information to the public, even through Congress or the courts
- Per DoDI 5230.29:
  - Prepublication review is NOT a declassification action
  - Anyone submitting material for prepublication review must believe it is unclassified prior to submission
  - Material submitted to DOPSR must first be coordinated and reviewed within the originating DoD Component

Student Guide

Unauthorized Disclosure Refresher

Lesson 4: Responding to Unauthorized Disclosure

Contents

Media Response

E-mail Notification: Media Inquiry

You just received another e-mail. It looks like it's from someone named Stephen Waters at XYZ news.

To: You
From: Stephen Waters, XYZ News
Subject: Information Request
Hi there,

A source sent me a link to a website where your organization is listed in connection with classified project specifications, timelines, and other details.

I think the public would be very interested in learning more about this and I was hoping you could confirm these details and provide your thoughts on the organization's projects.

Thanks,
Stephen

Mr. Waters is looking for information regarding a specific classified project. You are working on that project and know that many of the project specifications are Secret.

If you need help with the following series of questions, refer to the Hints table below.

Responding to Unauthorized Disclosure: Protect Information and Report the Incident – Hints

- If necessary, immediately safeguard classified material
  - Take personal possession of the classified material
  - Secure classified material in an approved security container, other approved area, or:
    - DoD: Provide the material to your Security Manager
    - Industry: Provide the material to your Facility Security Officer (FSO)
- For classified information suspected in the media or on the Internet:
  - Do NOT
    - View or download information
    - Make any comment that confirms or verifies information
    - Discuss information with anyone who does not have an appropriate security clearance and need-to-know
  - Do:

- Provide point of contact for media inquiries:
  - DoD: Refer all media to your Component's Public Affairs Office
  - Industry: Refer all media to your FSO

- When an Negligent Discharge of Classified Information (NDCI) or spill occurs:
  - Isolate and contain to:
    - Minimize damage (e.g. physically disconnect computer from the network)
    - Preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or counterintelligence purposes (e.g. do not delete the information)
- Verify with the Original Classification Authority (OCA) that the information is classified. The OCA will ensure a damage assessment is conducted, if necessary.
- Refer to DoDM 5200.01, Vol. 4 and/or other regulations/policies as necessary for handling unauthorized disclosure or spills involving Controlled Unclassified Information (CUI)
- Report any of the following to your Security Manager (DoD) or FSO (industry):
  - Suspected or actual incidents of unauthorized disclosure
  - Attempts to solicit classified information
  - Violations of security regulations

Media Response: Question 1

Stephen Waters, a reporter at XYZ news, sent you an e-mail inquiring about a potential leak of classified project information. How should you respond to Mr. Waters?

Decide how you want to proceed.

- ○ Forward the e-mail to your personal e-mail so you can respond to Mr. Waters without getting you or your organization into trouble with the media
- ○ Contact Mr. Waters and offer an exclusive interview
- ○ Contact Mr. Waters and confirm the existence of the classified projects listed but offer no additional details
- ○ Refer Mr. Waters to your organization's Public Affairs Office

Do not proceed to the next page until you select your response.

Media Response: Question 1 Answer

Correct Response: You should provide a point of contact for all media inquiries.

DoD employees should refer all media to their component's Public Affairs Office and industry employees should refer media to their FSO.

Media Response: Question 2

Now that you have referred him to the Public Affairs Office, should you delete the e-mail from Stephen Waters?

Decide how you want to proceed.

- ○ Yes. You should remove any evidence of a potential information leak.
- ○ No. You should preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or counterintelligence purposes.

Do not proceed to the next page until you select your response.

Media Response: Question 2 Answer

Correct Response: You should preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or counterintelligence purposes.

Media Response: Question 3

Do you want to visit the website to see whether there is, in fact, classified information on the site?

Decide how you want to proceed.

- ○ Yes. Before informing anyone of the incident you should visit the website to confirm that the website isn't a hoax.
- ○ No. You must not view or download any media from public sources that may contain classified information.

Do not proceed to the next page until you select your response.

Media Response: Question 3 Answer

Correct Response: For classified information suspected in the media or on the Internet you must NOT:

- View or download information
- Make any comment that confirms or verifies information
- Discuss information with anyone who does not have an appropriate security clearance and need-to-know

Media Response: Question 4

Should you take any additional action regarding Stephen Waters' e-mail?

Decide how you want to proceed.

- ○ Call 911 to inform your local law enforcement of the incident
- ○ Report the incident to the CIA
- ○ Report the incident to your Security Manager
- ○ No further action is required

Do not proceed to the next page until you select your response.

Media Response: Question 4 Answer

Correct Response: DoD employees should report any suspected or actual incidents of unauthorized disclosure, attempts to solicit classified information, or violations of security regulations to the Security Manager.

Industry employees should report such incidents to the FSO.

Next Steps

Call with Jonathan: Next Steps

Jonathan: Hi, this is Jonathan – we talked earlier today. I just got an e-mail from a reporter asking for information about a classified project! I referred him to the Public Affair's Office and reported the incident… but it got me thinking. What has to happen following an incident like this?

If you need help with the following series of questions, refer to the Hints tables below.

Steps in Responding to Unauthorized Disclosure: Overview – Hints

- Employees must:
  - Immediately protect the information
  - Report unauthorized disclosure
- Authorities must:
  - Investigate the incident
  - Impose sanctions
  - Report to Congress, if required
  - Conduct damage assessment

Steps in Responding to Unauthorized Disclosure: Reporting – Hints

Initial reporting:

- DoD:
  - Security Managers report incidents of unauthorized disclosure using the Security Incident Database (SID), the DoD-wide system for reporting serious security incidents
- Industry:
  - FSOs report incidents of unauthorized disclosure, loss, compromise, or suspected compromise of classified information (including NDCI incidents) to their Industrial Security Representatives (IS Reps) who:
    - Use the Industrial Security Facilities Database (ISFD) to track

security incidents
    - Notify the Government Contracting Activity (GCA)
  - FSOs report security incidents involving espionage to the Federal Bureau of Investigation (FBI)

Additional reporting requirements:

- Security managers and/or security officials must report classified data spills (NDCI) to appropriate authorities, including:
  - The OCA
  - The information owner/originator
  - The Information System Security Manager (ISSM)
  - The responsible computer incident response center
- DoD Components report serious security incidents to the Office of the Under Secretary of Defense for Intelligence [OUSD(I)], including any that involve:
  - Espionage
  - Unauthorized disclosure in the public media
  - Any incident where Congressional reporting may be required
  - Any actual or potential compromise involving sensitive compartment information (SCI) or special access programs (SAPs)
- Congressional reporting is required by OUSD(I) when unauthorized disclosure is likely to cause significant harm or damage to the national security
  - The OUSD(I) consults with the Director of National Intelligence (DNI) and the Director of the FBI, as appropriate, before submitting any such notification

Steps in Responding to Unauthorized Disclosure: Investigations and Damage Assessments – Hints

Inquiries and Investigations:

- For DoD incidents:
  - The component initiates the inquiry or investigation
  - If the chain of command is unclear, the OUSD(I) determines investigative primacy
  - The OUSD(I) consults with the Assistant Secretary of Defense (ASD) for Public Affairs to see if the information was officially released under proper authority
  - In NDCI cases, Component Security Managers and the commander

or senior official of the organization responsible receive copies of the inquiry or investigation report

- For incidents at cleared companies:
  - The FSO initiates an administrative inquiry to determine the cause and establish responsibility for the incident.
  - The FSO notifies IS Rep, who in turn, notifies the GCA, and other areas of Defense Security Service (DSS)
- Appropriate action will be taken to identify those responsible for unauthorized disclosure of CUI and corrective action and/or sanctions shall be taken or levied against those responsible

Damage Assessments:

- In response to unauthorized disclosure, the OCA, subject matter experts, and other security officials (as needed) conduct damage assessments to determine the effect of a compromise on national security

Next Steps: Question 1

Jonathan has reported the incident, but he would like to know more about how his organization responds to unauthorized disclosure. Which of the following will occur following unauthorized disclosure?

Answer Jonathan's question by selecting all that apply.

- ☐ Protect the information
- ☐ Report unauthorized disclosure to authorities
- ☐ Investigate incident
- ☐ Impose sanctions
- ☐ Conduct a damage assessment

Do not proceed to the next page until you select your response.

Next Steps: Question 1 Answer

Correct Response: All of these are steps that need to occur following an incident of unauthorized disclosure.

Next Steps: Question 2

Jonathan: So I reported this incident to the Component Security Manager. What happens next?

Decide how you want to respond to Jonathan.

- ○ The Security Manager will immediately report the potential unauthorized disclosure using the SID (the DoD-wide system for reporting serious security incidents)
- ○ The Security Manager will carry out a damage assessment
- ○ The Security Manager will do nothing at this point, but will collect all incidents to file in an annual report

Do not proceed to the next page until you select your response.

Next Steps: Question 2 Answer

Correct Response: The Security Manager will immediately report the potential unauthorized disclosure using the SID (the DoD-wide system for reporting serious security incidents).

Next Steps: Question 3

Jonathan: I know some very serious incidents must be reported to the Office of the Under Secretary of Defense for Intelligence. If this reporter writes up a story that contains classified information, will that be required?

Jonathan would like to know whether this incident will need to be reported to the OUSD(I).

Decide how you want to respond to Jonathan.

- ○ Yes. ALL incidents must be reported to OUSD(I).
- ○ Yes. DoD Components must report any incidents of unauthorized disclosure in the public media to OUSD(I).
- ○ No. Only espionage incidents must be reported to OUSD(I).

Do not proceed to the next page until you select your response.

Next Steps: Question 3 Answer

Correct Response: DoD Components report serious incidents to OUSD(I), including any that involve unauthorized disclosure in the public media.

Next Steps: Question 4

Jonathan: Do really serious incidents need to be reported anywhere else?

Jonathan would like to know whether serious incidents require any additional reporting.

Decide how you want to respond to Jonathan.

- ○ Yes. If unauthorized disclosure is likely to cause significant harm or damage to national security then Congressional reporting is required.
- ○ No. No additional reporting is required.

Do not proceed to the next page until you select your response.

Next Steps: Question 4 Answer

Correct Response: Congressional reporting is required when unauthorized disclosure is likely to cause significant harm or damage to national security.

The OUSD(I) consults with the DNI and the Director of the FBI, as appropriate, before submitting any such notification.

Next Steps: Question 5

Jonathan: So whose responsibility is it to start investigating the incident?

Jonathan would like to know who will initiate the inquiry and/or investigation.

Decide how you want to respond to Jonathan.

- ○ Jonathan and any other affected employees
- ○ The DoD Component
- ○ The FBI
- ○ Congress

Do not proceed to the next page until you select your response.

Next Steps: Question 5 Answer

Correct Response: For DoD, the Component initiates the inquiry or investigation. For cleared companies, the FSO initiates an administrative inquiry.

Next Steps: Question 6

Jonathan: Maybe the information on that website was actually authorized for release. Is there a process to check that?

Jonathan would like to know whether there is a process to determine if information in the public media was authorized for public release.

Decide how you want to respond to Jonathan.

- ○ Yes. The OUSD(I) consults with the ASD for Public Affairs to determine whether information was officially released under proper authority.
- ○ Yes. The OUSD(I) consults with the information originator to determine whether the information was officially authorized for release.
- ○ No. The OUSD(I) must investigate all information in the public media as if it were an information leak.

Do not proceed to the next page until you select your response.

Next Steps: Question 6 Answer

Correct Response: The OUSD(I) consults with the ASD for Public Affairs to see if the information was officially released under proper authority.

Next Steps: Question 7

Jonathan: And you said the last step was a damage assessment? What's the purpose of that?

Jonathan has asked about damage assessments. What is the purpose of this step in the response to unauthorized disclosure?

Decide how you want to respond to Jonathan.

- ○ Determine how much information was released, and to whom
- ○ Determine the best method to contain the unauthorized disclosure
- ○ Determine the effect of the compromise on national security

Do not proceed to the next page until you select your response.

Next Steps: Question 7 Answer

Correct Response: In response to unauthorized disclosure, the OCA, subject matter experts, and other security officials (as needed) conduct damage assessments to determine the effect of a compromise on national security.

How Did You Do?

Consider how you did on the questions in this lesson. If you need to review any of the information in more detail, refer to the appropriate Job Aid included below and on the following pages.

Responding to Unauthorized Disclosure – Job Aid

Overview

- Employees must:
  - Immediately protect the information
  - Report unauthorized disclosure
- Authorities must:
  - Investigate the incident
  - Impose sanctions
  - Report to Congress, if required
  - Conduct damage assessment

Protect Information

- If necessary, immediately safeguard classified material
  - Take personal possession of the classified material
  - Secure classified material in an approved security container, other approved area, or:
    - DoD: Provide the material to your Security Manager
    - Industry: Provide the material to your FSO
- For classified information suspected in the media or on the Internet:
  - Do NOT
    - View or download information
    - Make any comment that confirms or verifies information
    - Discuss information with anyone who does not have an appropriate security clearance and need-to-know
  - Do:
    - Provide point of contact for media inquiries:
      - DoD: Refer all media to your Component's Public

Affairs Office
    - Industry: Refer all media to your FSO
- When an NDCI or spill occurs:
    - Isolate and contain to:
        - Minimize damage (e.g. physically disconnect computer from the network)
        - Preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or counterintelligence purposes (e.g. do not delete the information)
- Verify with the OCA that the information is classified. The OCA will ensure a damage assessment is conducted, if necessary.
- Refer to DoDM 5200.01, Vol. 4 and/or other regulations/policies as necessary for handling unauthorized disclosure or spills involving CUI

Report the Incident

Initial reporting:

- DoD:
    - Security Managers report incidents of unauthorized disclosure using the Security Incident Database (SID), the DoD-wide system for reporting serious security incidents
- Industry:
    - FSOs report incidents of unauthorized disclosure, loss, compromise, or suspected compromise of classified information (including NDCI incidents) to their IS Reps who:
        - Use the ISFD to track security incidents
        - Notify the GCA
    - FSOs report security incidents involving espionage to the FBI

Additional reporting requirements:

- Security managers and/or security officials must report classified data spills (NDCI) to appropriate authorities, including:
    - The OCA
    - The information owner/originator
    - The ISSM
    - The responsible computer incident response center
- DoD Components report serious security incidents to the OUSD(I), including any that involve:
    - Espionage

- Unauthorized disclosure in the public media
- Any incident where Congressional reporting may be required
- Any actual or potential compromise involving SCI or SAPs

- Congressional reporting is required by OUSD(I) when unauthorized disclosure is likely to cause significant harm or damage to the national security
  - The OUSD(I) consults with the DNI and the Director of the FBI, as appropriate, before submitting any such notification

Investigate the Incident

- For DoD incidents:
  - The component initiates the inquiry or investigation
  - If the chain of command is unclear, the OUSD(I) determines investigative primacy
  - The OUSD(I) consults with the ASD for Public Affairs to see if the information was officially released under proper authority
  - In NDCI cases, Component Security Managers and the commander or senior official of the organization responsible receive copies of the inquiry or investigation report
- For incidents at cleared companies:
  - The FSO initiates an administrative inquiry to determine the cause and establish responsibility for the incident.
  - The FSO notifies IS Rep, who in turn, notifies the GCA, and other areas of DSS
- Appropriate action will be taken to identify those responsible for unauthorized disclosure of CUI and corrective action and/or sanctions shall be taken or levied against those responsible

Assess the Damage

- In response to unauthorized disclosure, the OCA, subject matter experts, and other security officials (as needed) conduct damage assessments to determine the effect of a compromise on national security

Student Guide

Unauthorized Disclosure Refresher

Lesson 5: Course Conclusion

Contents

Course Summary

Topic Review

It looks like you have come to the end of your eventful day, and completed all of your responsibilities. Here is a list of topics covered by the course:

- Misconceptions Regarding Unauthorized Disclosure
- Impacts of Unauthorized Disclosure
- Disclosure Authorization
- Prepublication Review
- Media Response
- Next Steps

If you found you did poorly in a particular area, you might want to review the job aid before taking the final exam.

Conclusion

Congratulations. You have completed the *Unauthorized Disclosure Refresher* course.

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

- Identify the types of unauthorized disclosure
- Recognize the impacts of unauthorized disclosure
- Demonstrate how to protect classified information and controlled unclassified information (CUI) to prevent unauthorized disclosure
- Determine actions to take if you learn of suspected or actual unauthorized disclosure

To receive course credit, you must take the *Unauthorized Disclosure Refresher* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.