Student Guide

Unauthorized Disclosure of Classified Information for DoD and Industry

Course Overview

Course Introduction

Course Overview

The scope of damage done to our collection capabilities from media disclosures of classified information is well documented. Hundreds of serious press leaks have significantly impaired U.S. capabilities against our hardest targets. The government report, *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, details several leaks that have collectively cost the American people hundreds of millions of dollars and have done grave harm to national security. Welcome to the Unauthorized Disclosure of Classified Information for DoD and Industry course.

Course Objectives

Because the United States Government has placed its trust in you, you have been given access to classified information. Whether you've had access to classified information for a long time or just received it in the past year, you know that when you protect classified information, you are protecting our nation's security along with the war fighters who defend the American way of life.

In this course, you will review what unauthorized disclosure of classified information is and the impacts of such disclosure. You will also review how to protect classified information and prevent unauthorized disclosure, the reporting requirements for suspected or actual incidents of unauthorized disclosure, and the penalties individuals who engage in unauthorized disclosure may face. Here are the course objectives.

- Identify types of unauthorized disclosure
- Recognize the impacts of unauthorized disclosure
- Identify how to protect classified information to prevent unauthorized disclosure
- Determine actions to take if you learn of suspected or actual unauthorized disclosure

Student Guide

Unauthorized Disclosure of Classified Information for DoD and Industry

Lesson 1: What Is Unauthorized Disclosure?

Introduction

Opening

There are so many examples of how unauthorized disclosure of classified information has disrupted U.S. missions related to national security. And you've got to wonder, you know….how can one person hide from the U.S. for so long? But the answer often comes back to this: unauthorized disclosure of classified information.

According to the *9/11 Commission Report*, the *Washington Times* published a story in 1998 that made reference to the U.S. using Bin Laden's satellite phone to track his movements and communications. The day after the article published, the phone went dark. Coincidence? Possibly. But more than likely it's not. Revealing a source and method in this case was potentially the reason the U.S. lost the ability to track Bin Laden.

Through similar media leaks, the U.S. lost track of Al Qaeda's network of sites, Obelisk, which had provided the U.S. information about operational communications between Al Qaeda elements. The media leaks also caused the U.S. to lose access to terrorist financial networks. The disclosure of this classified program led to a change in how terrorist financial networks operated, making it much more difficult to track and interrupt funding operations.

Objectives

In this lesson, you will review what constitutes unauthorized disclosure of classified information, including specific types of unauthorized disclosure and some common misconceptions about unauthorized disclosure.

You will also review the types of damage caused by unauthorized disclosure and the various sanctions you could face if caught engaging in unauthorized disclosure. Here are the lesson objectives:

- Identify types of unauthorized disclosure

- Recognize the impacts of unauthorized disclosure

Overview of Unauthorized Disclosure

Definition of Unauthorized Disclosure

As defined in DoDM 5200.01, Volume 3, DoD Information Security Program, unauthorized disclosure is the communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient. To understand who unauthorized recipients are, let's first review who authorized recipients of classified information are.

As a cleared employee, you should recall that authorized recipients must meet three requirements to access classified information. First, they must have a favorable determination of eligibility at the proper level for access to classified information. Second, they must have a "need-to-know" for access to classified information. And third, they must have signed an SF-312, Classified Information Nondisclosure Agreement (NDA), before accessing classified information. Therefore, if an individual has not met all three of these requirements, that individual would be considered an unauthorized recipient of classified information.

An unauthorized recipient can be anyone. They can be your friends or family members, acquaintances, coworkers, or even superiors within your agency, command, or company who may be appropriately cleared but don't have a need-to-know. They can be potential employers who see what you post on social network sites such as LinkedIn and Facebook. They can even be media outlets and foreign intelligence services. You never know whose hands such information will fall into.

Types of Unauthorized Disclosure

Unauthorized disclosure of classified information is a type of security incident that can be characterized as an infraction or violation depending on the seriousness of the incident. Unauthorized disclosure of classified information can happen in various ways. It can be disclosed either intentionally or accidentally and can occur through leaks, spills, espionage, or not following proper safeguarding procedures.

Leaks

Leaks are deliberate disclosures of classified information to the media. Well-known examples of leaks include leaks of information regarding top secret government surveillance programs to news outlets and Bradley Manning's leaks of hundreds of thousands of classified documents, such as diplomatic cables and U.S. Army reports, to the WikiLeaks website.

Spills

Classified data spills are accidental or intentional disclosures of classified information that occur across computer systems, such as when classified information from the SECRET internet protocol router network (SIPRNet) is opened on the non-secure internet protocol router network (NIPRNet). Spills are considered and handled as a possible compromise of classified information involving information systems, networks, and computer equipment until it is determined whether an unauthorized disclosure occurred.

The most common ways that spills happen are through email and Internet postings. The classified information could be in the body of the email, in an attachment to the email, or both. Even if individually all elements are unclassified, sometimes the compilation of the body of the email and the attachment results in disclosure of classified information.

Similarly, posting unclassified defense and U.S. Government information data elements to publicly accessible Internet sites can jeopardize militarily-relevant data because when compiled together the information could become classified, which is known as a classified compilation. Be careful what unclassified defense and U.S. Government information you send in an email and post on the Internet to avoid classified compilations for public access.

Espionage

Espionage includes activities designed to obtain, deliver, communicate, or transmit information relating to the national defense with the intent or reason to believe such information will be used to harm the United States or to the advantage of a foreign nation or transnational entity.

Improper Safeguarding Procedures

Unauthorized disclosure of classified information due to improper safeguarding procedures, although usually unintentional, can be just as damaging to national security as intentional unauthorized disclosures.

Examples of this type of unauthorized disclosure include, but are not limited to, leaving a classified document on a photocopier, forgetting to secure classified information before leaving your office, and discussing classified information in earshot of unauthorized recipients. Another example of this type of unauthorized disclosure relates to dual-use technology, or technology designed for both military and commercial use. Cleared employees must review information related to such technology prior to presenting it to commercial users to ensure it contains no classified information related to the military technology.

Misconceptions about Unauthorized Disclosure

Unauthorized Disclosure to News Media

With several high-profile cases of classified information being released to the media in recent years, let's look at some misconceptions about unauthorized disclosure of classified information to the news media and review the rules all cleared personnel must remember. If classified information has been put in the public domain, then it is okay for cleared employees to freely share it.

This is false! Even though classified information appears in the public domain, such as in a newspaper or on the Internet, it is still classified until an official declassification decision is made. Cleared personnel are legally bound not to view or share classified information in the public domain and may be subject to sanctions if they seek out such information, acknowledge its accuracy or existence, or disseminate the information in any way. If a cleared employee does view the information online, then it must be reported as a data spill, and the spill must be isolated and contained on the computer used to view it.

Here's another misconception about unauthorized disclosure to the media. Cleared employees who disclose classified information to a reporter or journalist may receive protection through "journalist's privilege," which allows reporters and journalists to protect their sources during grand jury proceedings.

This is also false! Cleared employees must remember they will not be afforded protection by "journalist's privilege" if they disclose classified information to a reporter or journalist. Journalists called to testify during grand jury proceedings must reveal their sources.

Limits on Protection for Cleared Employees

Two other common misconceptions about unauthorized disclosure of classified information are that cleared employees can receive protection under the Presidential Policy Directive 19 (PPD-19), Protecting Whistleblowers with Access to Classified Information or under the First Amendment. PPD-19 protects employees from direct retaliation for acts of reporting waste, fraud and abuse through proper channels. The First Amendment guarantees free speech but does not protect employees who disclose classified information unlawfully.

Impact of Unauthorized Disclosure

Damage Caused by Unauthorized Disclosure

Our country is harmed in many ways when someone discloses classified information without authorization. We suffer damage to our national security, which includes the undermining of ongoing and planned U.S. operations, damage to our intelligence community sources and methods, and detrimental effects on our international alliances and foreign policy. Unauthorized disclosure also benefits adversaries wishing to harm the U.S. Through unauthorized disclosure of classified information, our military and even civilian citizens suffer loss of life, our government and industry face financial costs, the public's confidence and trust in our government is eroded, and we all risk losing our way of life.

We won't always know exactly what the fallout is from each unauthorized disclosure. For example, Bradley Manning's leaks of classified information to the WikiLeaks website is considered to be one of the largest incidents of unauthorized disclosure in U.S. history, but we don't know yet what all of the repercussions are. However, we do know that the impacts of unauthorized disclosure are serious.

Levels of Classification

Classification levels are applied to classified information based on the level of damage that could reasonably be expected to be caused to national security if unauthorized disclosure of that information occurs. The unauthorized disclosure of Confidential information could reasonably be expected to cause damage to national security. The unauthorized disclosure of Secret information could reasonably be expected to cause serious damage to national security. The unauthorized disclosure of Top Secret information could reasonably be expected to cause exceptionally grave damage to national security.

Review Activity

Review Activity 1

You have a classified document you would like to share with your coworker, John. What requirements must John meet to be an authorized recipient of the classified information you wish to share with him?

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

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

Review Activity 2

Select True or False for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

	True	**False**
You heard that someone posted classified information on the Internet. Since you are a cleared employee, it is okay for you to view that information to see what the buzz is all about.	○	○
If you disclose classified information unlawfully to a reporter, you will not receive protection through "journalist's privilege" because reporters and journalists must disclose their sources in grand jury proceedings.	○	○
You viewed classified information posted in the public domain on your computer, but you do not have to report a data spill since you *inadvertently* viewed the information.	○	○

Review Activity 3

Select Top Secret, Secret, or Confidential for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

	Top Secret	**Secret**	**Confidential**
The unauthorized disclosure of this type of classified information is reasonably expected to cause exceptionally grave damage to national security.	○	○	○
The unauthorized disclosure of this type of classified information is reasonably expected to cause damage to national security.	○	○	○
The unauthorized disclosure of this type of classified information is reasonably expected to cause serious damage to national security.	○	○	○

Answer Key - Review Activities

Review Activity 1

You have a classified document you would like to share with your coworker, John. What requirements must John meet to be an authorized recipient of the classified information you wish to share with him?

Select all that apply.

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

***Feedback**: To be an authorized recipient of the classified information you wish to share with John, he must have a favorable eligibility determination for access to the level of classified information you wish to share, he must have signed a nondisclosure agreement (NDA), and he must have a need-to-know to access that information. It is important to remember that rank or seniority within an organization is not a factor in granting a person access to classified information.*

Review Activity 2

Select True or False for each statement.

	True	False
You heard that someone posted classified information on the Internet. Since you are a cleared employee, it is okay for you to view that information to see what the buzz is all about.	○	⊙
***Feedback**: Classified information in the public domain is classified until officially declassified. Therefore, you are subject to sanctions if you view, acknowledge, or disseminate the information in any way.*		

	True	False
If you disclose classified information unlawfully to a reporter, you will not receive protection through "journalist's privilege" because reporters and journalists must disclose their sources in grand jury proceedings.	⊙	○
***Feedback**: You will not be afforded protection by "journalist's privilege" if you disclose classified information to a reporter or journalist because sources must be disclosed in grand jury proceedings.*		
You viewed classified information posted in the public domain on your computer, but you do not have to report a data spill since you *inadvertently* viewed the information.	○	⊙
***Feedback**: If you view classified information posted in the public domain on your computer, either intentionally or inadvertently, then you must report a data spill, and the spill must be isolated and contained on the computer you used to view it.*		

Review Activity 3

Select Top Secret, Secret, or Confidential for each statement.

	Top Secret	Secret	Confidential
The unauthorized disclosure of this type of classified information is reasonably expected to cause exceptionally grave damage to national security.	⊙	○	○
The unauthorized disclosure of this type of classified information is reasonably expected to cause damage to national security.	○	○	⊙
The unauthorized disclosure of this type of classified information is reasonably expected to cause serious damage to national security.	○	⊙	○

Student Guide

Unauthorized Disclosure of Classified Information for DoD and Industry

Lesson 2: Preventing Unauthorized Disclosure

Introduction

Opening

We see headlines about classified information leaks far too often. Osama Bin Laden was very good at evading capture for many years. We had the information we needed to find him, but on more than one occasion someone leaked enough classified information for Bin Laden to continue hiding. Are you confident you are doing everything you can to prevent unauthorized disclosure of classified information?

Objectives

In this lesson, you will review how to protect classified information from unauthorized disclosure through proper classification and declassification procedures as well as through proper disclosure and safeguarding measures. Here is the lesson objective:

- Identify how to protect classified information to prevent unauthorized disclosure

Protecting Classified Information

As a cleared employee, you are required and have pledged to protect classified information by following proper classification procedures, applying downgrading and declassification instructions, physically safeguarding classified information, and complying with guidelines for engaging the news media and publishing information. These requirements were established by Executive Order 13526, Classified National Security Information, and are detailed in the DoDM 5200.01, DoD Information Security Program, Volumes 1 through 4, and DoD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM) for contractors cleared under the National Industrial Security Operating Program (NISP).

The Center for Development of Security Excellence (CDSE) offers in-depth training on these requirements in several eLearning courses as follows:

- Original Classification Course
- Marking Classified Information Course
- Derivative Classification Course
- Derivative Classification Refresher Course
- Downgrading and Declassification Short

Proper Classification and Declassification

Classification

Executive Order 13526 states that classified national security information must be properly classified. The Original Classification Authority (OCA) must initially determine what level of damage would occur if there were unauthorized disclosure of that classified information. As a cleared employee and potential derivative classifier, you must ensure proper classification markings appear on all classified information when creating a new classified document based on one or more authorized sources. In addition, derivative classifiers must take the Derivative Classification Refresher training every two years.

Downgrading and Declassification

After assigning an overall classification level based on the highest level of information a document contains, the OCA specifies downgrading and declassification dates, events, and exemptions to protect information as long as necessary at its designated classification level. Derivative classifiers must protect classified information from unauthorized disclosure by ensuring that the appropriate classification, downgrading, and declassification instructions are respected and carried forward from one or more authorized sources to a newly created classified document. Authorized sources include the Security Classification Guide, properly marked source documents, and DD Form 254, Department of Defense Contract Security Classification Specification.

Safeguarding Classified Information

Safeguarding Classified Information

Executive Order 13526, DoDM 5200.01, and the NISPOM provide guidance for safeguarding classified information from unauthorized disclosure. Each and every day, it is your responsibility to follow this guidance to protect classified information from unauthorized disclosure. You must properly handle classified information, including the use of classified cover sheets when classified information is outside of a GSA-approved container. You must store classified information in GSA-approved security containers or other approved methods as stated in DoDM 5200.01, Volume 3, or the NISPOM, when you are not handling the information. You must follow guidelines for the reproduction of classified information, which include using only

copiers designated specifically for reproducing classified information, and for the transmission and transportation of classified information, which include very specific hand carry procedures. And when you destroy classified information, you must follow the disposal and destruction guidelines, which outline authorized destruction methods, such as shredding, depending on the type of media to be destroyed. Remember, you are required to protect classified information throughout your life, even after you are no longer an employee.

The Center for Development of Security Excellence (CDSE) offers in-depth training on these requirements in several eLearning courses as follows:

- Classified Storage Requirements Short
- Transmission and Transportation for DoD Course
- Transmission and Transportation for Industry Course
- Safeguarding Classified Information in the NISP Course
- Disposal and Destruction Short

Social Media and News Media

In all areas of your life, you must be mindful of your obligation to protect classified information and prevent its unauthorized disclosure. DoD Manual 5200.01 states that when using social networking services, which include, but are not limited to Facebook, Twitter, YouTube, MySpace, wikis, and blogs, the requirements for protecting classified information from unauthorized disclosure and the penalties for ignoring those requirements are the same as when using other media and methods of dissemination. Also, remember, the news media does not have a favorable determination of eligibility for access to classified information and does not have a need-to-know for classified information, nor has the news media signed an SF-312. Therefore, you should never publicly acknowledge the release of classified information and you must be careful not to make any statement or comment that confirms the accuracy of or verifies information requiring protection. You should refer all media to your Component's Public Affairs Office which is the official channel for DoD.

Prepublication Review

As a cleared employee—including when you are no longer an employee— you may write books, articles, speeches, and briefings, but if they contain official DoD information, then there are certain rules you must follow before those items may be publicly released. As outlined in DoD Directive (DoDD) 5230.09, Clearance of DoD Information for Public Release, you must submit the materials to the Defense Office of Prepublication and Security Review for a prepublication review to ensure they do not contain any classified information before submitting them for public release. You

must also believe that the information you are submitting for prepublication review is unclassified information.

Public release includes sending any book, manuscript, or article to a publisher, editor, movie producer, or game purveyor, or their respective support staffs. Public release also includes distributing any speech, briefing, article, or content that will be publicly available, even if the release to the public is through Congress or the courts. It is important to remember that prepublication review is not a declassification action.

Review Activities

Review Activity 1

Properly classifying information aids in preventing unauthorized disclosure. Indicate who performs each classification function. Then check your answers in the Answer Key at the end of this Student Guide.

	Original Classification Authority	**Derivative Classifier**
Carries forward classification, downgrading and declassification instructions	○	○
Initially determines what level of damage would occur if there were unauthorized disclosure of that classified information	○	○
Specifies downgrading and declassification dates, events, and exemptions	○	○

Review Activity 2

You are a cleared DoD employee. Select True or False for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

	True	**False**
If Congress requests that you disclose official DoD information, you must submit that information for prepublication review before disclosing to Congress.	○	○
You may answer any questions from the news media regarding official DoD information as long as that information is not classified.	○	○
If you wish to write a memoir, you must submit any classified information for a prepublication review, so that it may be declassified.	○	○

Answer Key - Review Activities

Review Activity 1

Properly classifying information aids in preventing unauthorized disclosure. Indicate who performs each classification function.

	Original Classification Authority	**Derivative Classifier**
Carries forward classification, downgrading and declassification instructions	○	⊙
***Feedback**: Derivative classifiers carry forward classification, downgrading and declassification instructions set forth by the OCA.*		
Initially determines what level of damage would occur if there were unauthorized disclosure of that classified information	⊙	○
***Feedback**: The OCA makes the initial determination what level of damage would be expected to occur if there were unauthorized disclosure of that classified information to determine what classification level to apply to that information.*		
Specifies downgrading and declassification dates, events, and exemptions	⊙	○
***Feedback**: The OCA specifies downgrading and declassification dates, events, and exemptions to protect information as long as necessary at its designated classification level.*		

Review Activity 2

You are a cleared DoD employee. Select True or False for each statement.

	True	False
If Congress requests that you disclose official DoD information, you must submit that information for prepublication review before disclosing to Congress.	⊙	○
***Feedback**: You must submit any official DoD information you wish to disclose to the public, including disclosure through Congress, for a prepublication review prior to submission.*		
You may answer any questions from the news media regarding official DoD information as long as that information is not classified.	○	⊙
***Feedback**: You must never engage the news media unless through official channels, which is the Public Affairs office for DoD employees.*		
If you wish to write a memoir, you must submit any classified information for a prepublication review, so that it may be declassified.	○	⊙
***Feedback**: While it is true that you must submit your memoir for prepublication review, you must never submit classified information for a prepublication review. Prepublication review is not a declassification action.*		

Student Guide

Unauthorized Disclosure of Classified Information for DoD and Industry

Lesson 3: Responding to Unauthorized Disclosure

Introduction

Opening

Thanks to diligent reporting, the consequences of unauthorized disclosure can be blunted. Take the example of former hacker, Adrian Lamo, who reported Bradley Manning to the FBI. If Mr. Lamo hadn't notified the FBI that Manning told him he had access to thousands of classified documents and provided Lamo details about his relationship with WikiLeaks, who knows how much more damage could have been done to the U.S. The WikiLeaks case shows how more incremental damage can be done. And it's people like Mr. Lamo who do the right thing to stop the bad guys.

Objectives

You know what constitutes unauthorized disclosure of classified information. But do you know what to do if you see or suspect unauthorized disclosure? In this lesson, you will review the steps that you and others must take in response to unauthorized disclosure of classified information. Here is the lesson objective:

- Determine actions to take if you learn of suspected or actual unauthorized disclosure

How to Respond to Unauthorized Disclosure

Overview of Steps

Once you discover or suspect unauthorized disclosure, you must first protect the classified information to prevent further unauthorized disclosure. Then you must report the unauthorized disclosure to the appropriate authorities who will, in turn, investigate the incident and impose sanctions, if warranted. The incident may need to be reported to Congress, under certain circumstances, and a damage assessment must be conducted. Let's take a look at each of these steps more closely.

Protect Classified Information

The first thing you must do if you see or suspect unauthorized disclosure of classified information is to protect it from further unauthorized disclosure. If you find classified material that has been left unattended, immediately protect it by taking personal possession of the material and securing it in a GSA approved security container.

If you see or hear about something in the media or on the Internet that you suspect is classified information, do not make any comment that confirms the accuracy of or verifies the information in question or discuss with anyone who does not have the appropriate security clearance and need-to-know. Also, do not view or download the information.

If the media contacts you, you may provide a point of contact for their inquiries. For DoD, that point of contact is the Public Affairs Office.

If a classified data spill occurs, you must isolate and contain the spill to minimize the damage. To do this, disconnect your computer from the network. Do not delete anything from your computer or erase the hard drive because you must preserve the evidence for damage assessment, risk assessment, and law enforcement or counterintelligence purposes. You should secure the computer in a GSA-approved security container or approved storage area to prevent unauthorized access until further action to remove the classified data is warranted.

Finally, verify with the information owner that the information is classified. If the information is classified, the information owner will also ensure that a damage assessment is conducted, if necessary.

Report Unauthorized Disclosure

The next step in your response to actual or suspected unauthorized disclosure is to report the incident. If you are a DoD employee, report the incident to your security manager. If you are a cleared contractor, report the incident to your Facility Security Officer (FSO) who will, in turn, report it to your company's Defense Security Service Industrial Security Representative (DSS IS Rep).

DoD security managers use the DoD-wide system for reporting and managing serious security incidents to report these incidents and then are able to track their investigations and associated actions.

DSS IS Reps use the Industrial Security Facilities Database (ISFD) to track security incidents, including unauthorized disclosure security incidents, at cleared contractor facilities. Also, through their field office, IS Reps notify the Government Contracting Activity (GCA) of security incidents.

Additional Reporting Requirements

Once the incident has been reported, there are still further reporting requirements for the following types of unauthorized disclosure incidents: data spills, incidents that must be reported to the Office of the Under Secretary of Defense for Intelligence [OUSD(I)] and incidents that must be reported to Congress.

Data Spill Reporting

DoD security managers must report classified data spills and other security incidents through their agency's chain of command to the appropriate authorities, which include the Original Classification Authority (OCA); the information owner or originator, if other than the OCA; the Information System Security Manager (ISSM) and the responsible computer incident response center. IS Reps track data spills through the Industrial Security Facilities Database and through their field office to the GCA.

Reporting to OUSD(I)

All serious security incidents must be reported to the OUSD(I) if they involve espionage, unauthorized disclosure to the public media or any incident where Congressional reporting may be required, or any compromise of our most sensitive information, such as Sensitive Compartmented Information (SCI) or Special Access Programs (SAPs). Security incidents involving the following must be reported to OUSD(I):

- Espionage
- Unauthorized disclosure to the public media
- Unauthorized disclosure that:
    - Is reported to the oversight committees of Congress
    - May attract significant public attention
    - Involves large amounts of classified information
    - Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices
- Special Access Programs (SAPs)
    - Actual or potential compromises
    - Vulnerabilities in SAP policy or procedures that lead to actual or potential compromise
    - Security failure or unauthorized disclosure

Other security incidents that must be reported to OUSD(I) are those:

- Relating to any defense operation, system, or technology
- Likely to cause significant harm or damage to U.S. national security
- For which Congressional reporting may be required

OUSD(I) must also receive reports of egregious security incidents as determined by the DoD Component senior agency official and security incidents involving unauthorized disclosure of Sensitive Compartment Information (SCI). If SCI is under control of an Intelligence Community agency other than DoD, it must also be reported to National Counterintelligence Executive who will notify the other agency.

Reporting to Congress

Some unauthorized disclosures are so serious or of such interest to the public that DoD must report them to Congress. After consulting with the Director of National Intelligence (DNI) and the Director of the Federal Bureau of Investigation (FBI), the OUSD(I) must report to Congress on behalf of the Secretary of Defense each security or counterintelligence failure or compromise of classified information that the Secretary determines is likely to cause significant harm or damage to the national security. The Secretary of Energy must report to Congress each security incident involving unauthorized disclosure of restricted data and/or formerly restricted data.

Investigate Incident

After you report a security incident, an inquiry is launched.

For DoD incidents, the Component initiates the investigation. When responsibility for an inquiry into an unauthorized public media disclosure is unclear, the security manager refers the matter through his or her chain of command to the Office of the Under Secretary of Defense for Intelligence [OUSD(I)] who, in turn, determines which Component has investigative primacy. The OUSD(I) consults with the Assistant Secretary of Defense (ASD) for Public Affairs, if the DoD Component hasn't already, to see whether the information was officially released under proper authority.

For cleared companies, the FSO initiates an administrative inquiry to determine the cause and establish responsibility for the unauthorized disclosure. The FSO also notifies the DSS IS Rep, who in turn, notifies the GCA, and other areas of DSS.

Impose Sanctions

Those who are responsible for unauthorized disclosure face serious consequences. After the investigation is conducted, sanctions may be imposed against the individual. These consequences can take the form of Uniform Code of Military Justice (UCMJ) sanctions, civil litigation, administrative sanctions, and criminal sanctions. You'll recall that many of these sanctions were imposed on Bradley Manning as a result of his unauthorized disclosure to WikiLeaks.

Conduct Damage Assessment

The OCA and subject matter experts, along with security officials, as needed, conduct a damage assessment in response to unauthorized disclosure in espionage cases and leaks to the public media to determine the effect of a compromise on national security.

Review Activities

Review Activity 1

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

If you suspect unauthorized disclosure of classified information, what should you do first?

- ○ Conduct an investigation to determine if it really is unauthorized disclosure
- ○ Protect the classified information from further unauthorized disclosure
- ○ Conduct a damage assessment
- ○ Report what you suspect

Review Activity 2

Select True or False for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

	True	**False**
A damage assessment should only be conducted when the incident must be reported to Congress.	○	○
Some people go to prison when convicted of unauthorized disclosure of classified information.	○	○
As a cleared contractor employee, you should report any incident you suspect of being unauthorized disclosure to your FSO, even if you're not 100% sure it's unauthorized disclosure.	○	○

Answer Key - Review Activities

Review Activity 1

Select the best response.

If you suspect unauthorized disclosure of classified information, what should you do first?

- ○ Conduct an investigation to determine if it really is unauthorized disclosure
- ⊙ Protect the classified information from further unauthorized disclosure
- ○ Conduct a damage assessment
- ○ Report what you suspect

***Feedback**: If you suspect unauthorized disclosure of classified information, you should you should first protect the classified information from further unauthorized disclosure, then report what you suspect.*

Review Activity 2

Select True or False for each statement.

	True	False
A damage assessment should only be conducted when the incident must be reported to Congress.	○	⊙
***Feedback**: A damage assessment must be conducted for all incidents of unauthorized disclosure to determine the effect of a compromise on national security.*		
Some people go to prison when convicted of unauthorized disclosure of classified information.	⊙	○
***Feedback:** There are many penalties for engaging in unauthorized disclosure of classified information, including, but not limited to, loss of pay, loss of rank, loss of job, and even incarceration.*		
As a cleared contractor employee, you should report any incident you suspect of being unauthorized disclosure to your FSO, even if you're not 100% sure it's unauthorized disclosure.	⊙	○
***Feedback**: Cleared contractor employees should report all suspected or actual incidents of unauthorized disclosure to their Facility Security Officer, who in turn will report the incidents to the IS Rep.*		

Student Guide

Unauthorized Disclosure of Classified Information for DoD and Industry

Lesson 4: Course Conclusion

Course Conclusion

Course Summary

In this course, you reviewed your responsibilities for protecting classified information from unauthorized disclosure. You also reviewed how to respond to suspected and actual incidents of unauthorized disclosure as well as the penalties for individuals who engage in unauthorized disclosure.

Course Objectives

Congratulations. You have completed the Unauthorized Disclosure of Classified Information for DoD and Industry course. You should now be able to:

- Identify types of unauthorized disclosure
- Recognize the impacts of unauthorized disclosure
- Identify how to protect classified information to prevent unauthorized disclosure
- Determine actions to take if you learn of suspected or actual unauthorized disclosure
- Identify the eight suitability factors and seven additional considerations used in suitability adjudications

To receive course credit, you MUST take the Unauthorized Disclosure of Classified Information for DoD and Industry examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.