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, not only of classified information, but also of Controlled Unclassified Information, or CUI.

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, 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:
Unauthorized Disclosure of Classified Information for DoD and Industry
Lesson 1: What Is Unauthorized Disclosure?

- 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.

Controlled unclassified information, or CUI, is unclassified information which requires safeguarding or dissemination controls in accordance with applicable laws, regulations, and government policies. Although a personnel security clearance is not required to access CUI, dissemination of and access to CUI requires practice of need-to-know principles and may be subject to additional limitations, such as unique transmission requirements or export controls.

CUI includes but is not limited to information designated as:

- For Official Use Only (FOUO)
- Law Enforcement Sensitive (LES),
- LIMITED DISTRIBUTION (LIMDIS)

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 can involve either classified information or CUI. When classified information is involved, unauthorized disclosure can be categorized as a
Unauthorized Disclosure of Classified Information for DoD and Industry
Lesson 1: What Is Unauthorized Disclosure?

Unauthorized disclosure 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 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**

Data spills are willful, negligent, or inadvertent disclosures of information. They occur when classified information or CUI is transferred or transmitted onto a system that lacks the appropriate security level or, in the case of CUI, that lacks the required protection or access controls. For example, if classified information from the secure internet protocol router network, or SIPRNet, is opened on the non-secure internet protocol router network, or NIPRNet, then a spill has occurred.

Spills like this can create the potential for widespread unauthorized disclosure of information in a relatively short amount of time. The impacts of these spills can be so severe when classified information is involved that a new term is applied: Negligent Discharge of Classified Information, or NDCI, which is based on the familiar firearms term “Negligent Discharge” to connote its seriousness.

Until it can be determined whether an unauthorized disclosure occurred, NDCIs are considered and handled as a possible compromise of classified information involving information systems, networks, and computer equipment.

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 CUI and other 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 of what CUI and other unclassified defense and U.S. Government information you send in an email and post on the Internet to avoid classified compilations for public access.
Remember that CUI may not be posted to publicly-accessible websites, and different types of CUI may require additional posting restrictions.

**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 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. 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.

Employees must also be aware that some types of CUI, such as export-controlled technical data, is subject to additional access restrictions and they must follow applicable regulations and access controls to prevent unauthorized disclosure. See Enclosure 3 of DoD Manual 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information, for additional details on protecting, transmitting, and safeguarding the various categories of CUI.
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 personnel must remember.

If classified information or CUI has been put in the public domain, then it is okay for employees to freely share it.

This is false! Even though classified information or CUI appears 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 is made, or in the case of CUI, it is no longer designated as such. 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 an 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! 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 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, 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.*

<table>
<thead>
<tr>
<th>Statement</th>
<th>True</th>
<th>False</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>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.</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Viewing For Official Use Only (FOUO) information posted online in the local domain is not a cause for concern since FOUO information is unclassified.</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th></th>
<th>Top Secret</th>
<th>Secret</th>
<th>Confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>The unauthorized disclosure of this type of classified information is reasonably expected to cause exceptionally grave damage to national security.</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>The unauthorized disclosure of this type of classified information is reasonably expected to cause damage to national security.</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>The unauthorized disclosure of this type of classified information is reasonably expected to cause serious damage to national security.</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th></th>
<th>True</th>
<th>False</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>☐</td>
<td>☑</td>
</tr>
</tbody>
</table>

**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.
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.

Viewing For Official Use Only (FOUO) information posted online in the local domain is not a cause for concern since FOUO information is unclassified.

**Feedback:** Viewing For Official Use Only (FOUO) information posted online in the local domain IS a cause for concern. Even though FOUO information is unclassified, it is still CUI and requires safeguarding.

**Review Activity 3**

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

<table>
<thead>
<tr>
<th></th>
<th>Top Secret</th>
<th>Secret</th>
<th>Confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>The unauthorized disclosure of this type of classified information is reasonably expected to cause exceptionally grave damage to national security.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>The unauthorized disclosure of this type of classified information is reasonably expected to cause damage to national security.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>The unauthorized disclosure of this type of classified information is reasonably expected to cause serious damage to national security.</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>