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. 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. 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 an unauthorized disclosure of classified information, 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. Under certain circumstances, the incident may need to be reported to

Congress or, for industry, to the GCA, and a damage assessment may need to 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 or, if you don't have access to a security container, provide the material to your security officer.

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 your component's Public Affairs Office.

If a classified data spill, or NDCI, 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 Original Classification Authority, or OCA, 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, or NDCI, 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, or DNCI incidents, and other security incidents through their agency's chain of command to the appropriate authorities, which include the 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 Compartmented 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 inquiry or 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.

In cases of classified data spills, or NDCI, once the inquiry or investigation is complete, the Component Security Manager and the commander or senior official of the organization responsible for causing the spillage also receive copies of the inquiry or investigation report. This report will also indicate whether the spill was willful, negligent, or inadvertent.

- Willful: A willful spill or disclosure is caused by a purposeful disregard of DoD security or information safeguarding policies or requirements.
- Negligent: A negligent spill or disclosure is caused by unreasonable actions.

- Inadvertent: An inadvertent spill or disclosure occurs when the individual did not know, and had no reasonable way of knowing, that the security violation or unauthorized disclosure was occurring.

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, commanders and supervisors may consider and impose a wide range of sanctions and actions against those found responsible for unauthorized disclosure of classified information. These consequences can take the form of Uniform Code of Military Justice (UCMJ) sanctions, civil litigation, administrative sanctions, and criminal sanctions. For example, individuals found responsible for NDCI may have their user accounts suspended and only reinstated after completion of remedial training. You'll recall that many of these sanctions were imposed on Bradley Manning as a result of his unauthorized disclosure of classified information to WikiLeaks.

Organizations are also subject to consequences and sanctions. The component found responsible for NDCI may be responsible for cleanup costs to restore networks affected by NDCI.

Although no formal security inquiry or investigation is required for unauthorized disclosure of CUI, every effort must be taken to identify those responsible, and these individuals may face similar administrative, civil, and criminal penalties. For more information on handling unauthorized disclosure or spillage of CUI, refer to DoDM 5200.01, Volume 4 and any other applicable laws or federal regulations.

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. Damage assessments may also be conducted for other types of compromises.

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 it to Congress

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 it to Congress

***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 is conducted as necessary for incidents of unauthorized disclosure and other compromises 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 their DSS IS Rep.*		