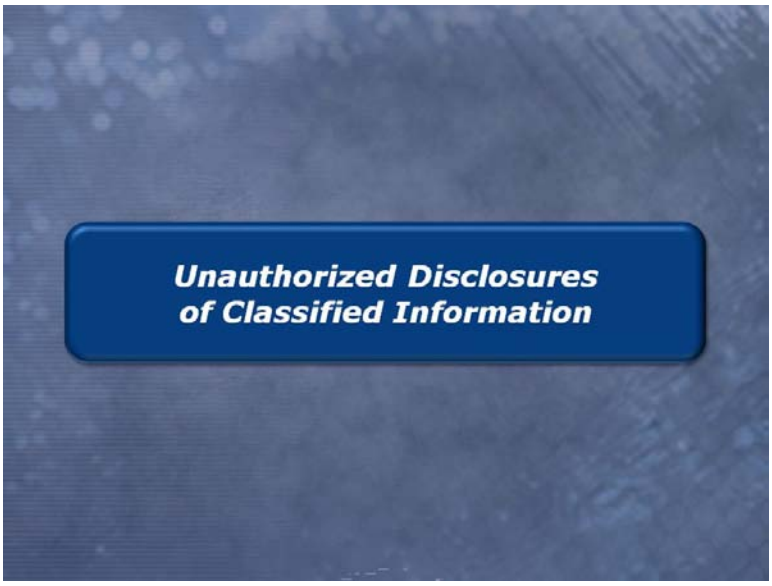
Unauthorized Disclosures of Classified Information
Text Alternative

The Office of the Director of National Intelligence (ODNI)
Office of the National Counterintelligence Executive (ONCIX)

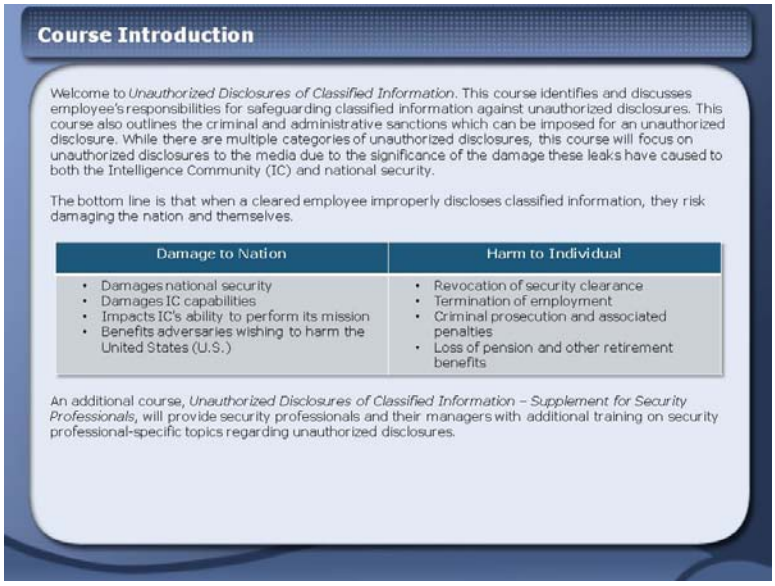
Last updated: September 2011

Contents

Unauthorized Disclosures of Classified Information 1
Course Introduction 2
Course Organization 3
Lesson 1: Defining Unauthorized Disclosures 4
Lesson 2: Harm Resulting from Unauthorized Disclosures 16
Lesson 3: Misconceptions and Employee Responsibilities 30
Topic 3.1: Misconceptions Related to Unauthorized Disclosures 30
Topic 3.2: Employee Responsibilities and Accountability 38
Course Summary 61
Additional Information 62



Unauthorized Disclosures of Classified Information



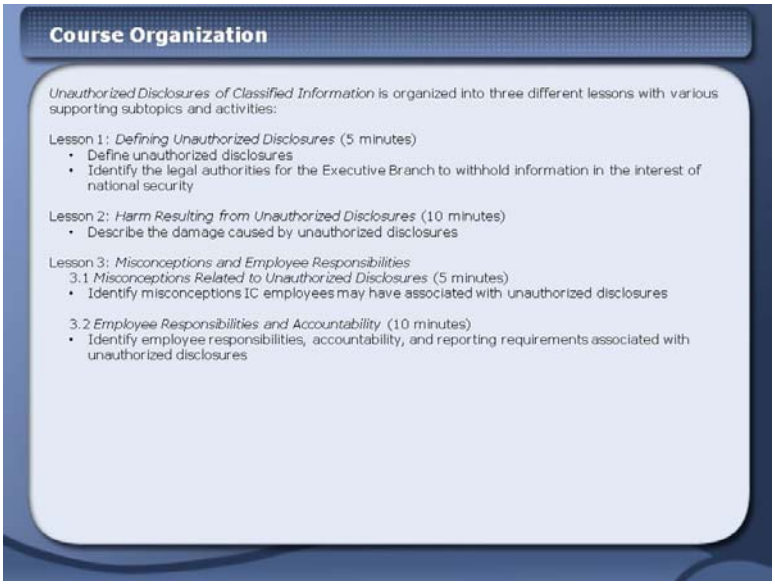
Course Introduction

Welcome to *Unauthorized Disclosures of Classified Information*. This course identifies and discusses employees' responsibilities for safeguarding classified information against unauthorized disclosures. This course also outlines the criminal and administrative sanctions which can be imposed for an unauthorized disclosure. While there are multiple categories of unauthorized disclosures, this course will focus on unauthorized disclosures to the media due to the significance of the damage these leaks have caused to both the Intelligence Community (IC) and national security.

The bottom line is that when a cleared employee improperly discloses classified information, they risk damaging the nation and themselves.

Damage to Nation	Harm to Individual
• Damage to national security • Damage to IC capabilities • Impact IC's ability to perform its mission • Benefit adversaries wishing to harm the United States (U.S.)	• Revocation of security clearance • Termination of employment • Criminal prosecution and associated penalties • Loss of pension and other retirement benefits

An additional course, *Unauthorized Disclosures of Classified Information – Supplement for Security Professionals*, will provide security professionals and their managers with additional training on security professional-specific topics regarding unauthorized disclosures.



Course Organization

Unauthorized Disclosures of Classified Information is organized into three different lessons with various supporting subtopics and activities:

Lesson 1: *Defining Unauthorized Disclosures* (5 minutes)

- Define unauthorized disclosures
- Identify the legal authorities for the Executive Branch to withhold information in the interest of national security

Lesson 2: *Harm Resulting from Unauthorized Disclosures* (10 minutes)

- Describe the damage caused by unauthorized disclosures

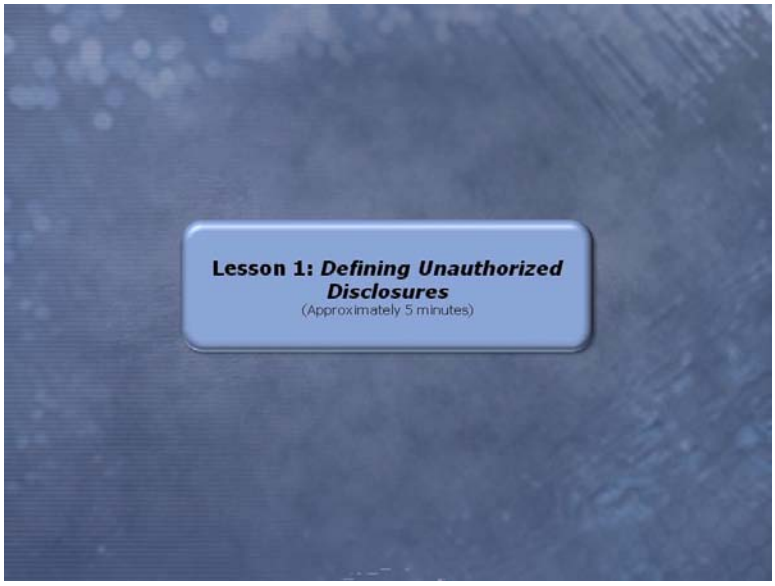
Lesson 3: *Misconceptions and Employee Responsibilities*

3.1 *Misconceptions Related to Unauthorized Disclosures* (5 minutes)

- Identify misconceptions IC employees may have associated with unauthorized disclosures

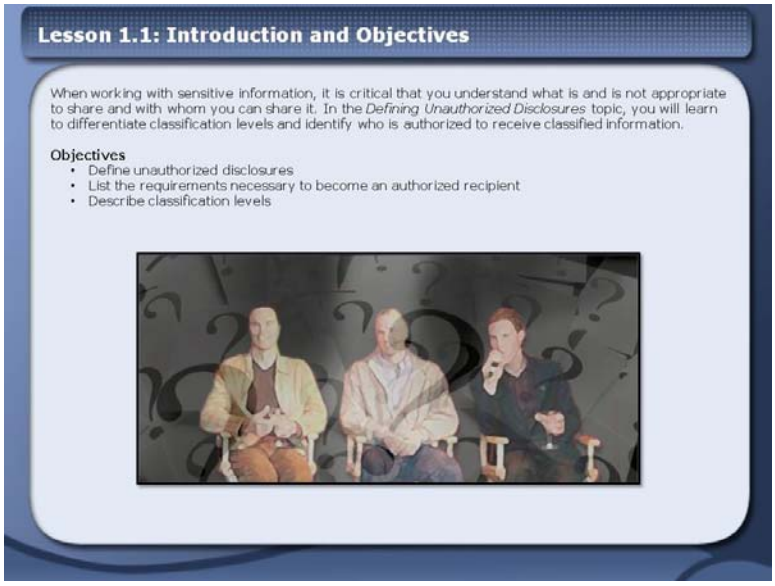
3.2 *Employee Responsibilities and Accountability* (10 minutes)

- Identify employee responsibilities, accountability, and reporting requirements associated with unauthorized disclosures



Lesson 1: Defining Unauthorized Disclosures

(Approximately 5 minutes)

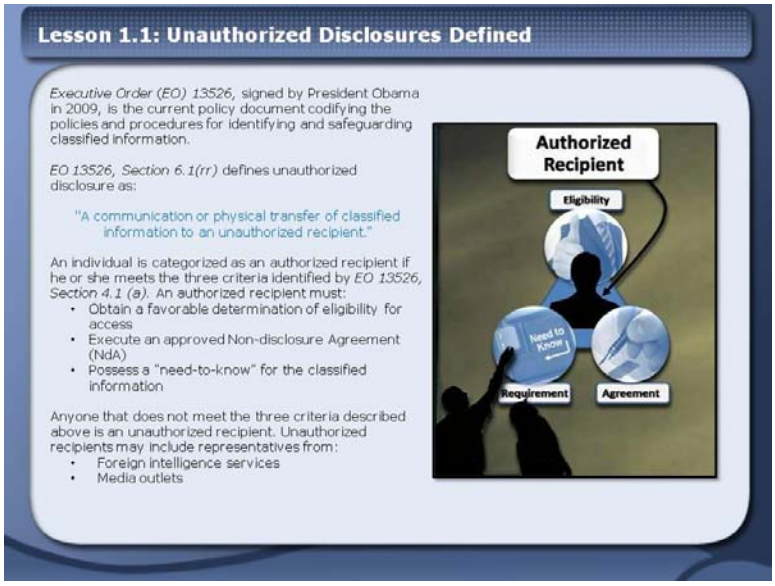


Lesson 1.1: Introduction and Objectives
When working with sensitive information, it is critical that you understand what is and is not appropriate to share and with whom you can share it. In the *Defining Unauthorized Disclosures* topic, you will learn to differentiate classification levels and identify who is authorized to receive classified information.

Objectives

- Define unauthorized disclosures
- List the requirements necessary to become an authorized recipient of classified information
- Describe classification levels

(Image Alt: Three unknown men sitting in chairs)



Lesson 1.1: Unauthorized Disclosures Defined
Executive Order (*EO) 13526,* signed by President Obama in 2009, is the current policy document codifying the policies and procedures for identifying and safeguarding classified information.

EO 13526, Section 6.1 (rr) defines authorized disclosure as:

Quote:
"A communication or physical transfer of classified information to an unauthorized recipient."

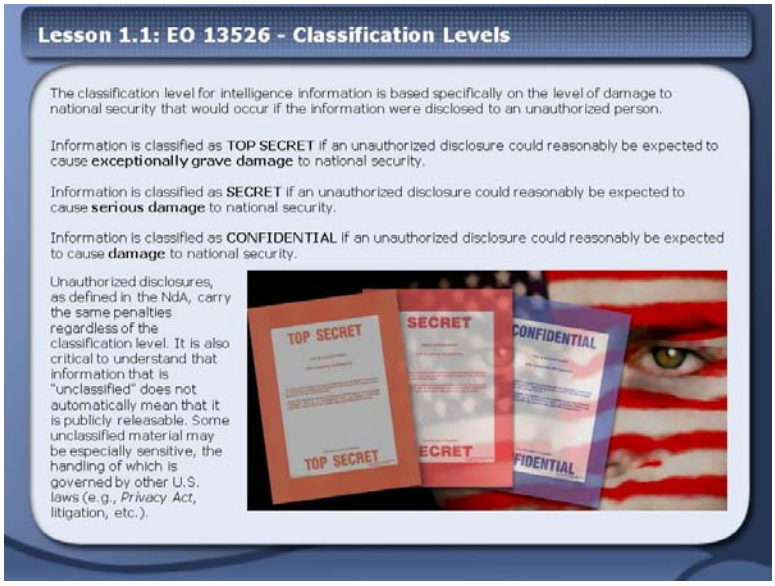
An individual is categorized as an authorized recipient if he or she meets the three criteria identified by *EO 13526, Section 4.1 (a).* An authorized recipient must:

- Obtain a favorable determination of eligibility for access
- Execute an approved Non-disclosure Agreement (NdA)
- Possess a "need-to-know" for the classified information

Anyone that does not meet the three criteria described above is an unauthorized recipient. Unauthorized recipients may include representatives from:

- Foreign intelligence services
- Media outlets

(Image Alt: Three criteria for an authorized recipient – "Eligibility" is a thumbs-up, "Requirement" is a "Need-to-Know" key on a keyboard, and "Agreement" is a signature on an NdA.)



Lesson 1.1: EO 13526 - Classification Levels
The classification level for intelligence information is based specifically on the level of damage to national security that would occur if the information were disclosed to an unauthorized person.

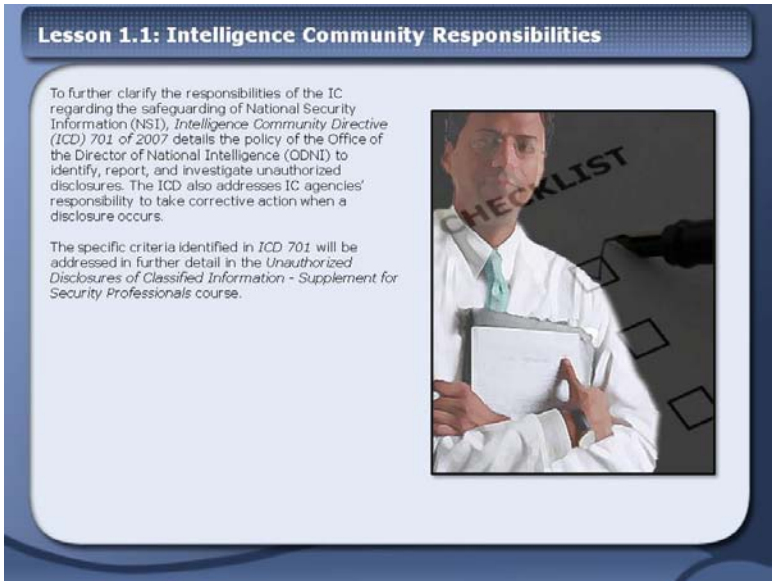
Information is classified as **TOP SECRET** if an unauthorized disclosure could reasonably be expected to cause **exceptionally grave damage** to national security.

Information is classified as **SECRET** if an unauthorized disclosure could reasonably be expected to cause **serious damage** to national security.

Information is classified as **CONFIDENTIAL** if an unauthorized disclosure could reasonably be expected to cause **damage** to national security.

Unauthorized disclosures, as defined in the NdA, carry the same penalties regardless of the classification level. It is also critical to understand that information that is “unclassified” does not automatically mean that it is publicly releasable. Some unclassified material may be especially sensitive, the handling of which is governed by other U.S. laws (e.g., *Privacy Act*, litigation, etc.).

(Image Alt: A collage of three classified documents, an American flag, and a face.)

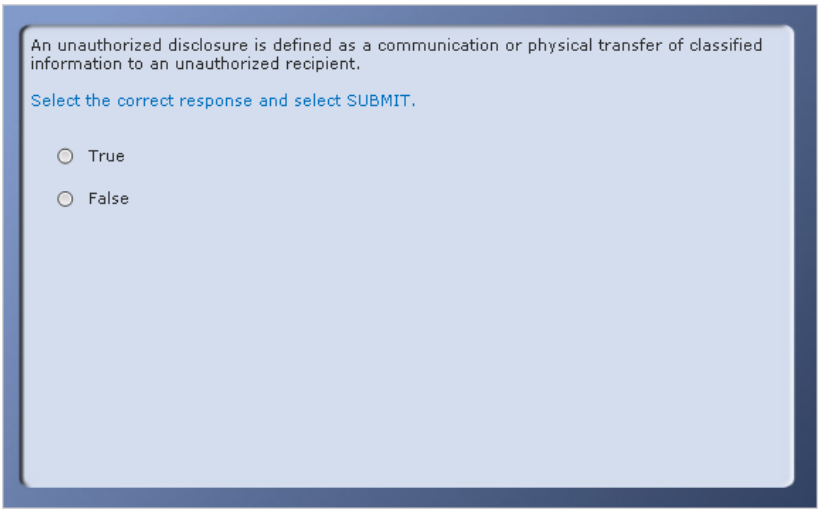


Lesson 1.1: Intelligence Community Responsibilities
To further clarify the responsibilities of the IC regarding the safeguarding of National Security Information (NSI), *Intelligence Community Directive (ICD) 701 of 2007* details the policy of the Office of the Director on National Intelligence (ODNI) to identify, report, and investigate unauthorized disclosures. The ICD also addresses IC agencies' responsibility to take corrective action when a disclosure occurs.

The specific criteria identified in *ICD 701* will be addressed in further detail in the *Unauthorized Disclosures of Classified Information - Supplement for Security Professionals* course.

(Image Alt: A collage of a man holding a clipboard and a checklist.)

Lesson 1.1: Knowledge Check



1. **An unauthorized disclosure is defined as a communication or physical transfer of classified information to an unauthorized recipient.**

Select the correct response and select SUBMIT.

a) True
b) False

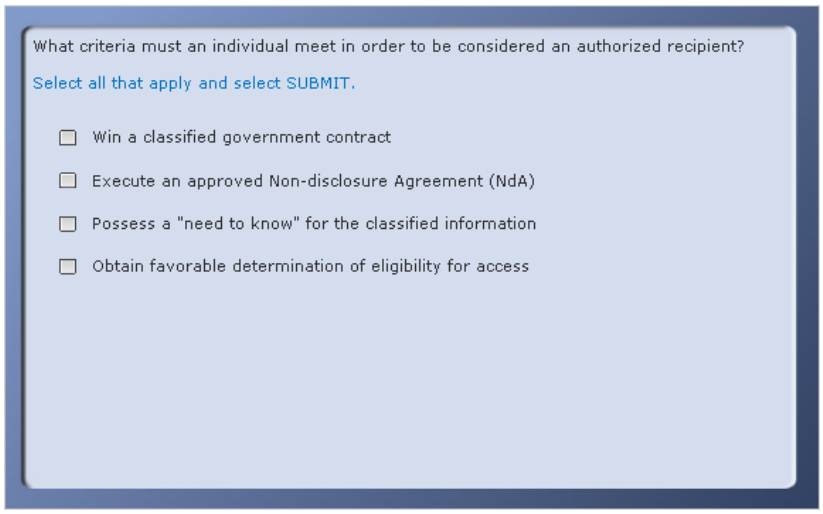
Correct Response:
True

Feedback when correct:
That's right! You selected the correct response.

Unauthorized disclosure is defined by *Executive Order (EO) 13526, Section 6.1(rr)*.

Feedback when incorrect:
You did not select the correct response. The correct response is True.

Unauthorized disclosure is defined by *Executive Order (EO) 13526, Section 6.1(rr)*.



2. What criteria must an individual meet in order to be considered an authorized recipient?

Select all that apply and select SUBMIT.

a) Win a classified government contract
b) Execute an approved Non-disclosure Agreement (NdA)
c) Possess a "need to know" for the classified information
d) Obtain favorable determination of eligibility for access

Correct Responses:

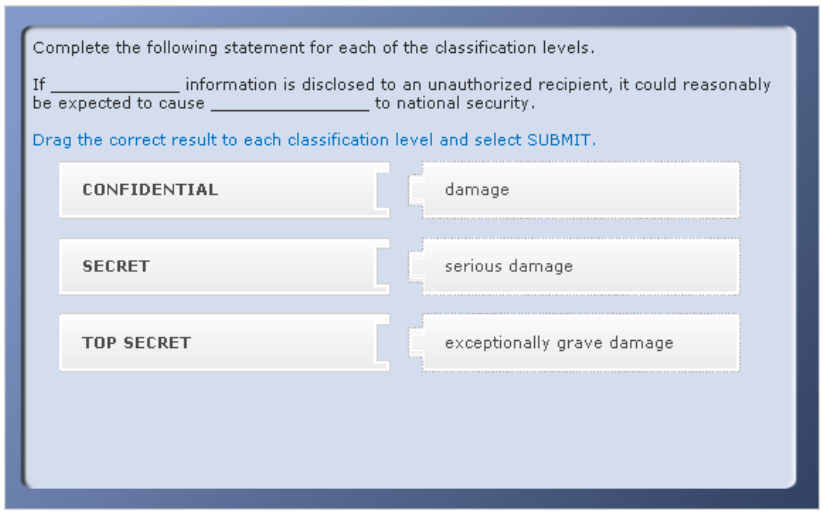
b) Execute an approved Non-disclosure Agreement (NdA)
c) Possess a "need to know" for the classified information
d) Obtain favorable determination of eligibility for access

Feedback when correct:
That's right! You selected the correct responses.

Feedback when incorrect:
You did not select the correct responses.

An authorized recipient must first:

- Obtain favorable determination of eligibility for access
- Possess a "need to know" for the classified information
- Execute an approved Non-disclosure Agreement (NdA)



3. Complete the following statement for each of the classification levels.

If _____ information is disclosed to an unauthorized recipient, it could reasonably be expected to cause _____ to national security.

Drag the correct result to each classification level and select SUBMIT.

Classification Levels:

a) **CONFIDENTIAL**
b) **SECRET**
c) **TOP SECRET**

Results:

a) damage
b) exceptionally grave damage
c) serious damage

Correct Responses:
If **CONFIDENTIAL** information is disclosed to an unauthorized recipient, it could reasonably be expected to cause **damage** to national security.

If **SECRET** information is disclosed to an unauthorized recipient, it could reasonably be expected to cause **serious damage** to national security.

If **TOP SECRET** information is disclosed to an unauthorized recipient, it could reasonably be expected to cause **exceptionally grave damage** to national security.

Feedback when correct:
That's right! You selected the correct responses.

Feedback when incorrect:
You did not select the correct responses.

The correct responses are:
If **CONFIDENTIAL** information is disclosed to an unauthorized recipient, it could reasonably be expected to cause **damage** to national security.

If **SECRET** information is disclosed to an unauthorized recipient, it could reasonably be expected to cause **serious damage** to national security.

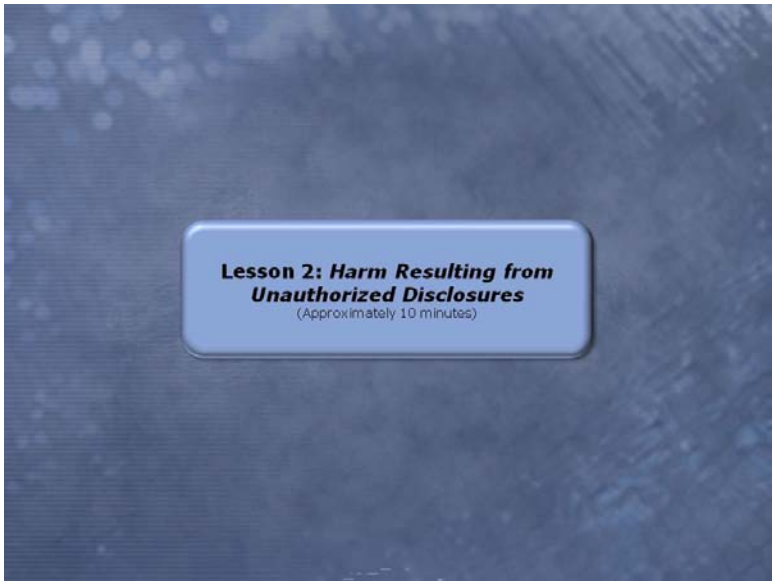
If **TOP SECRET** information is disclosed to an unauthorized recipient, it could reasonably be expected to cause **exceptionally grave damage** to national security.

Lesson 1: Summary
Sharing classified information with an individual who is not authorized to receive it is considered an unauthorized disclosure. You are responsible for safeguarding classified information. This means that you must be diligent about protecting information and identifying and immediately reporting any issues to the appropriate official in your agency or company.

There are three classification levels based on the level of damage to national security that would occur if the information were disclosed to an unauthorized person. It is vital that you understand your agency's requirements involving the transfer or release of National Security Information (NSI).

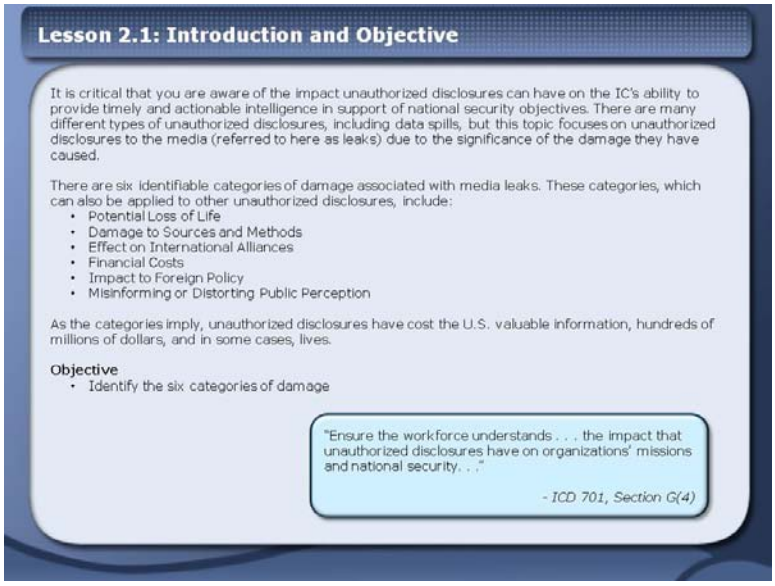
Now that you understand the definition of an unauthorized disclosure and your responsibilities for safeguarding classified NSI, let us explore the damage that is caused when an unauthorized disclosure occurs.

(Image Alt: Various security measures (e.g., security sticker, security guard, cipher lock, shredded paper, circuit board.))



Lesson 2: Harm Resulting from Unauthorized Disclosures

(Approximately 10 minutes)



Lesson 2.1: Introduction and Objective

It is critical that you are aware of the impact unauthorized disclosures can have on the IC's ability to provide timely and actionable intelligence in support of national security objectives. There are many different types of unauthorized disclosures, including data spills, but this topic focuses on unauthorized disclosures to the media (referred to here as leaks) due to the significance of the damage they have caused.

There are six identifiable categories of damage associated with media leaks. These categories, which can also be applied to other unauthorized disclosures, include:

- Potential Loss of Life
- Damage to Sources and Methods
- Effect on International Alliances
- Financial Costs
- Impact to Foreign Policy
- Misinforming or Distorting Public Perception

As the categories imply, unauthorized disclosures have cost the U.S. valuable information, hundreds of millions of dollars, and in some cases, lives.

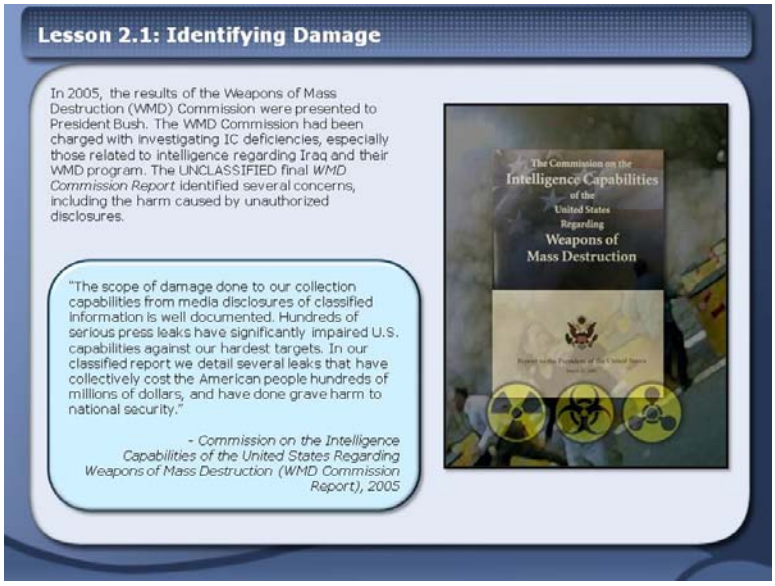
Objective

- Identify the six categories of damage

Call Out Box:

"Ensure the workforce understands . . . the impact that unauthorized disclosures have on organizations' missions and national security. . ."

~ICD 701, Section G(4)



Lesson 2.1: Identifying Damage
In 2005, the results of the Weapons of Mass Destruction (WMD) Commission were presented to President Bush. The WMD Commission had been charged with investigating IC deficiencies, especially those related to intelligence regarding Iraq and their WMD program. The unclassified final *WMD Commission Report* identified several concerns, including the harm caused by unauthorized disclosures.

Call Out Box:
"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. In our classified report we detail several leaks that have collectively cost the American people hundreds of millions of dollars, and have done grave harm to national security."

~Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission Report), 2005

(Image Alt: Collage of an emergency scene, the cover of the *WMD Commission Report*, and radiological symbols.)

Lesson 2.1: Categories of Damage
Introduction
There are six categories of damage to national security.
Select the arrow in the top right corner to learn more about these categories before proceeding.

Damage to Sources and Methods
When classified information is disclosed to unauthorized persons, the resultant damage extends beyond the specific information disclosed. These disclosures can give adversaries insight into the sources and methods used by the U.S. to collect information. Based on this knowledge, adversaries can take steps to either deny these collection efforts or take advantage of them and attempt to deceive the U.S. as to their true capabilities or intentions.

Potential Loss of Life
Intelligence collected from human sources (Human Intelligence or HUMINT) is particularly vulnerable to damage by unauthorized disclosure. Unfortunately, unauthorized disclosures of classified information by the media have been directly linked to the deaths of several individuals.

Effect on International Alliances
Unauthorized disclosures have had a negative impact on U.S. alliances with foreign partners by creating an atmosphere of distrust between the U.S. and foreign governments.

In addition to international alliances with foreign governments, disclosures can also damage the relationship between the IC and allied intelligence services. This has the potential to lead to agencies being less willing to collaborate with the U.S. IC in the future.

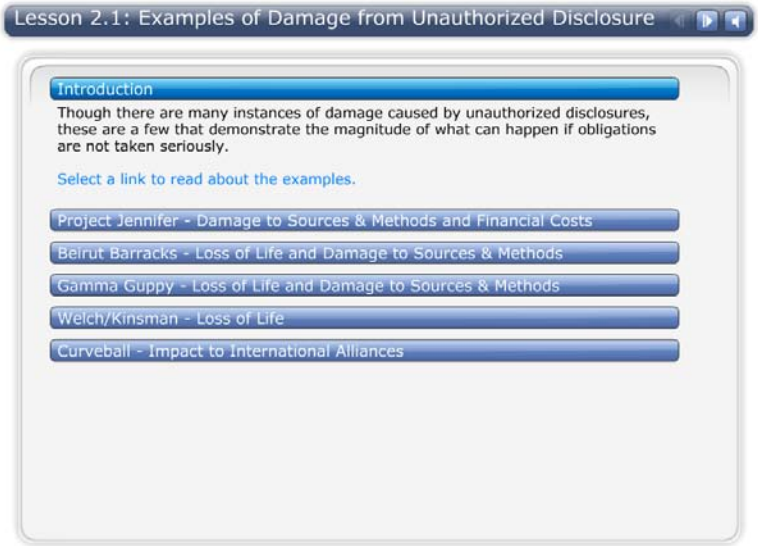
Financial Costs
Damage to the IC and national security caused by unauthorized disclosures can be measured in terms of financial loss. According to the unclassified *WMD Commission Report*, disclosures have collectively cost the American public hundreds of millions of dollars.

Impact to Foreign Policy

Unauthorized disclosures negatively impact foreign policy, including both the deliberation necessary to shape national policy as well as the implementation of approved policies.

Distorting Public Perception
In almost all cases of unauthorized disclosures, the public is only provided partial information. When this occurs, incorrect conclusions may be drawn based on the available information. Because the information is incomplete, the public actually may be **less** informed of the actions that the government is taking on their behalf. Since the government is unlikely to disclose additional classified information to clarify a previous unauthorized disclosure, the public is left with only partial information with which to form an opinion.

(Image Alt: Six arrows labeled with each category showing a schematic, coffins, a foreign national, money, flags, and a statistical pie graph.)



Lesson 2.1: Examples of Damage from Unauthorized Disclosure
Introduction
Though there are many instances of damage caused by unauthorized disclosures, these are a few that demonstrate the magnitude of what can happen if obligations are not taken seriously.
Select a link to read about the examples.

Project Jennifer - Damage to Sources & Methods and Financial Costs
Background: In the early 1970s, under a project with the code name "Project Jennifer," the U.S. was attempting to salvage a Soviet submarine that had sunk in the Pacific Ocean. Former Director of Central Intelligence (DCI) William Colby believed the successful recovery of the submarine would have been “the biggest single intelligence coup in history.” After the media discovered the existence of the operation, DCI Colby was able to convince several media outlets not to publish the information. Ultimately, the information was disclosed to the public when one media outlet refused Colby’s request.

Result: Based on the Times article and other disclosures in the U.S. media, the Soviets were able to send surveillance vessels to the salvage site, reportedly leading to the premature discontinuation of the operation. This project is reported to have cost $550 million, including $200 million to build the ship, “Glomar Explorer,” which had been specifically designed to salvage the submarine. After the disclosure, the ship was unable to participate in future intelligence operations.

(Image Alt: Collage on newspaper articles and Soviet hammer and sickle.)

Beirut Barracks - Loss of Life and Damage to Sources & Methods
Background: In April 1983, a television network and a newspaper reported that the U.S. was intercepting encrypted communications to Iran from a terrorist group in Syria.
Result: These communications were discontinued shortly after the disclosure. This undermined efforts to capture the terrorist leaders and eliminated a source of information about future attacks. In October 1983, 241 U.S. servicemen were killed when terrorists attacked the Marine Corps barracks in Beirut, Lebanon. The same terrorist group from whom the communications were intercepted is reported to have been responsible for the attack at the Marine Corps barracks. What cannot be known is if the

attack could have been prevented if the intelligence from the intercepted communications had not been lost.

(Image Alt: Cover of *Time* magazine with headline, “Carnage in Beirut.”)

Gamma Guppy - Loss of Life and Damage to Sources & Methods
Background: Under an effort with the code name "Gamma Guppy," the U.S. exploited its capability to intercept communications from the limousines of senior officials within the Soviet government. In 1971, the *Washington Post* disclosed this capability with a headline that read “CIA Eavesdrops on Kremlin Chiefs.”

Result: After the article was published, the Soviets began encrypting the conversations so that additional information was inaccessible. In addition, the Central Intelligence Agency (CIA) reportedly lost contact with an asset who had worked as a mechanic on the limousines. He was never heard from again and presumed killed.

(Image Alt: Collage of newspaper article and Soviet limousine.)

Welch/Kinsman - Loss of Life
Background: In 1969, Philip Agee, a former Case Officer, resigned from the CIA, moved out of the country, and began his campaign to weaken the CIA because of his ideological differences with the mission of the agency. As part of his campaign against the CIA, Agee was determined to expose CIA activity outside the U.S., including identifying CIA employees assigned overseas. An early 1975 edition of the magazine, Counterspy, published an article which included the following quote from Agee, “The most effective and important systematic attempts to combat the CIA that can be undertaken right now are, I think, the identification, exposure, and neutralization of its people working abroad.” In the same issue of Counterspy, Richard Welch was identified as the CIA’s Chief of Station (COS) in Greece. On November 25th, a Greek newspaper, the Athens Daily, also published Welch's identity. In 1980, the magazine, Covert Action Bulletin, also with a reported affiliation to Philip Agee, revealed the identities of 15 CIA officials working in Jamaica.

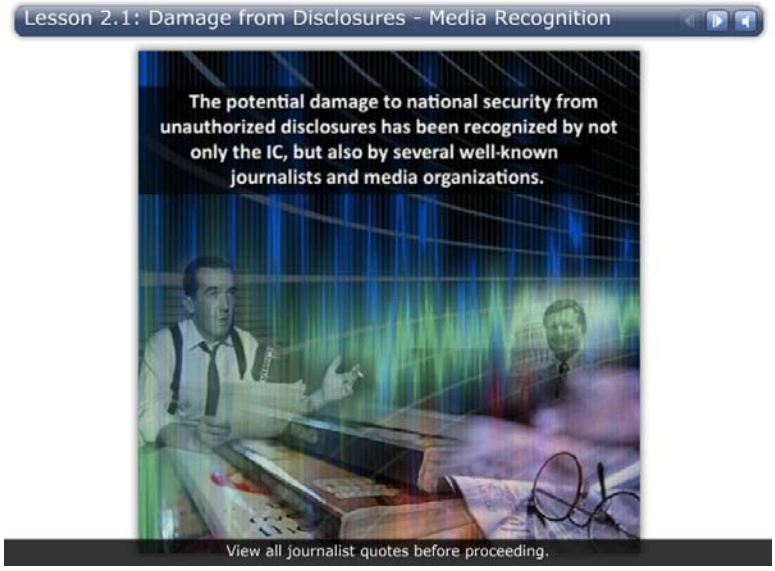
Result: On December 24, 1975, just one month after the article was published in the Athens Daily; COS Richard Welch was assassinated outside of his home in Athens. In 1980, just two days after the Covert Action Bulletin article was published, an attempt was made on the life of Richard Kinsman, who had been identified as the COS in Jamaica. Agee ultimately settled in Cuba, where he ran a travel agency until his death. He never returned to the U.S. after he began disclosing information about the identities of CIA employees and their activities

(Image Alt: Newspaper article with images of Richard Welch.)

Curveball - Impact to International Alliances
Background: Prior to the U.S. invasion of Iraq, “Curveball” was recruited by an allied foreign intelligence service to provide information regarding the status of Iraq's WMD program. As later explained in the WMD Commission Report, the allied intelligence service refused a request from the U.S. IC for direct access to Curveball for fear that his identity would be leaked. As it turned out, the information provided by Curveball was later determined not to be credible.

Result: Because the U.S. did not have direct access to Curveball, the IC was unable to directly assess his credibility and the accuracy of his information. This contributed to the analytical inaccuracies related to the status of Iraq's WMD program. Ultimately, Curveball's identity was disclosed by the U.S. media. This action potentially strained the political relationship between the U.S. and its ally, possibly threatening future collaboration.

(Image Alt: Collage of *60 Minutes* expose and images of Curveball.)



Lesson 2.1: Damage from Disclosures – Media Recognition
The potential damage to national security from unauthorized disclosures has been recognized by not only the IC, but also by several well-known journalists and media organizations.

(Image Alt: Collage of Walter Cronkite, Jack Nelson, and sound waves.)

Quote:
"Some leaks can endanger national security. We recognize that the government has a legitimate interest in protecting our national security secrets...Investigating and prosecuting those who leak information that causes harm is understandable."

~Tom Brokaw, Walter Cronkite, and Ted Koppel (May 2006)

(Image Alt: Collage of Ted Koppel, Walter Cronkite, and Tom Brokaw.)

Quote:
"Newspapers recognize that the government has a duty to preserve national security and that some leaks may cause damage."

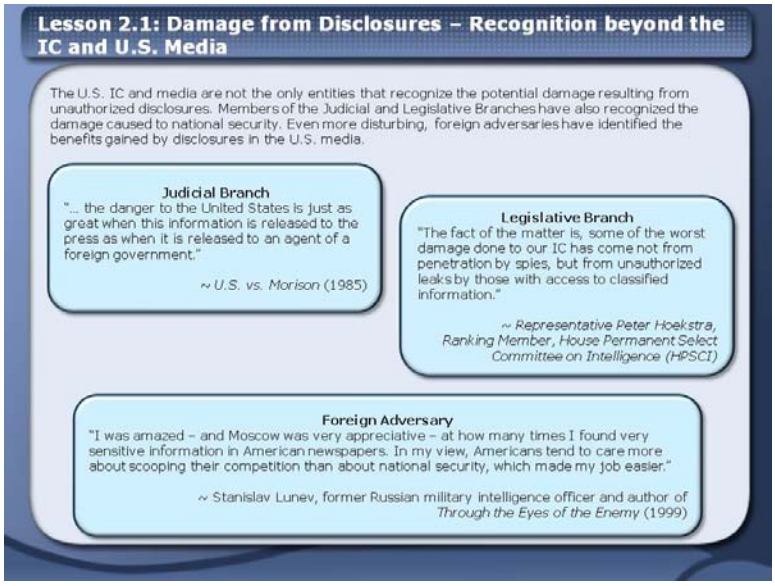
~Newspaper Association of America and National Newspaper Association (May 2006)

(Image Alt: Collage of newspapers, the Newspaper Association of America logo, and the National Newspaper Association logo.)

Quote:
"You may recall that in April 1983, some 60 people were killed in a bomb attack on the U.S. embassy in Beirut. At the time, there was coded radio traffic between Syria, where the operation was being run, and Iran, which was supporting it. Alas, one television network and a newspaper columnist reported that the U.S. government had intercepted the traffic. Shortly thereafter the traffic ceased. This undermined efforts to capture the terrorist leaders and eliminated a source of information about future attacks. Five months later, apparently the same terrorists struck again at the Marine barracks in Beirut; 241 servicemen were killed."

~Katherine Graham, Chief Executive Officer (CEO), *Washington Post* (April 1986)

(Image Alt: Collage of a *Newsweek* magazine featuring Katherine Graham, the *Washington Post* building, a *Washington Post* headline, and a young Katherine Graham.)



Lesson 2.1: Damage from Disclosures – Recognition beyond the IC and U.S. Media
The U.S. IC and media are not the only entities that recognize the potential damage resulting from unauthorized disclosures. Members of the Judicial and Legislative Branches have also recognized the damage caused to national security. Even more disturbing, foreign adversaries have identified the benefits gained by disclosures in the U.S. media.

Call Out Box:
Judicial Branch
"… the danger to the United States is just as great when this information is released to the press as when it is released to an agent of a foreign government."

~*U.S. vs. Morison* (1985)

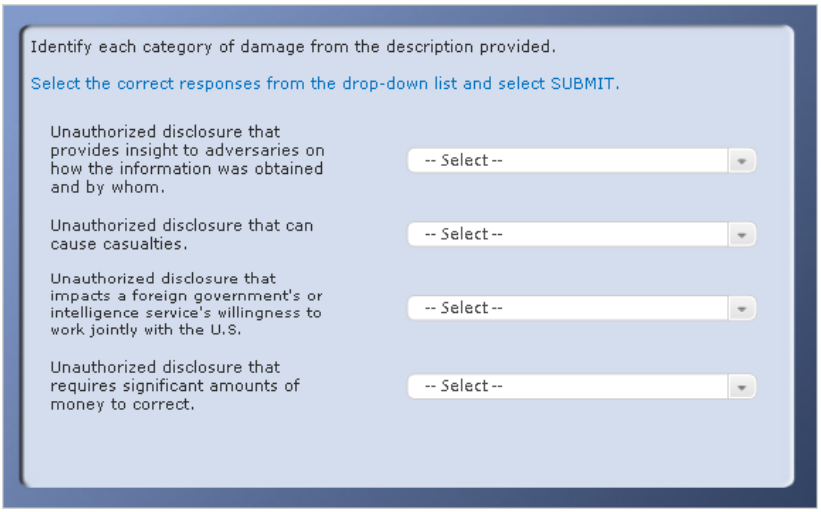
Call Out Box:
Legislative Branch
"The fact of the matter is, some of the worst damage done to our IC has come not from penetration by spies, but from unauthorized leaks by those with access to classified information."

~Representative Peter Hoekstra, Ranking Member, House Permanent Select Committee on Intelligence (HPSCI)

Call Out Box:
Foreign Adversary
"I was amazed – and Moscow was very appreciative – at how many times I found very sensitive information in American newspapers. In my view, Americans tend to care more about scooping their competition than about national security, which made my job easier."

~Stanislav Lunev, former Russian military intelligence officer and author of *Through the Eyes of the Enemy* (1999)

Lesson 2.1: Knowledge Check



1. Identify each category of damage from the description provided.

Select the correct responses from the drop-down list and select SUBMIT.

Descriptions:

a) Unauthorized disclosure that provides insight to adversaries on how the information was obtained and by whom.
b) Unauthorized disclosure that can cause casualties.
c) Unauthorized disclosure that impacts a foreign government’s or intelligence service's willingness to work jointly with the U.S.
d) Unauthorized disclosure that requires significant amounts of money to correct.

Category of Damage:

Damage to Sources and Methods
Effect on International Alliances
Financial Costs
Potential Loss of Life

Correct Responses:

a) Unauthorized disclosure that provides insight to adversaries on how the information was obtained and by whom. - Damage to Sources and Methods
b) Unauthorized disclosure that can cause casualties. - Potential Loss of Life
c) Unauthorized disclosure that impacts a foreign government's or intelligence service's willingness to work jointly with the U.S. - Effect on International Alliances
d) Unauthorized disclosure that requires significant amounts of money to correct. - Financial Costs

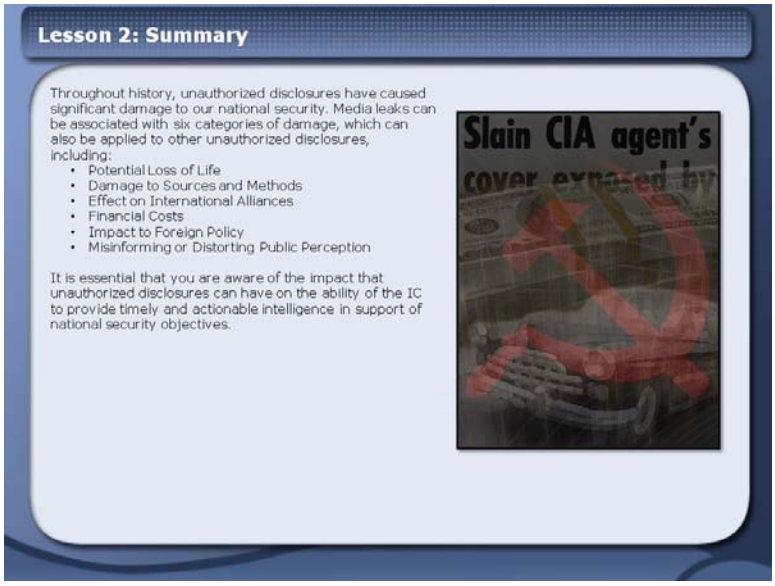
Feedback when correct:
That's right! You selected the correct responses.

The other two categories of damage are the Impact to Foreign Policy and the Distortion of Public Perception.

Feedback when incorrect:
Sorry, you did not select the correct responses.

There are six categories of damage - their descriptions are shown here. Though not all may be applicable in every instance, each is an impact associated with unauthorized disclosures.

- Damage to Sources and Methods is an unauthorized disclosure that provides insight to adversaries on how the information was obtained and by whom.
- Potential Loss of Life is an unauthorized disclosure that can cause casualties.
- Effect on International Alliances is an unauthorized disclosure that impacts a foreign government's or intelligence service's willingness to work jointly with the U.S.
- Financial Costs is an unauthorized disclosure that requires significant amounts of money to correct.
- Impact to Foreign Policy is an unauthorized disclosure that may damage political relationships, negatively effecting the creation and implementation of foreign policy.
- Distorting Public Perception is an unauthorized disclosure that influences public opinion.



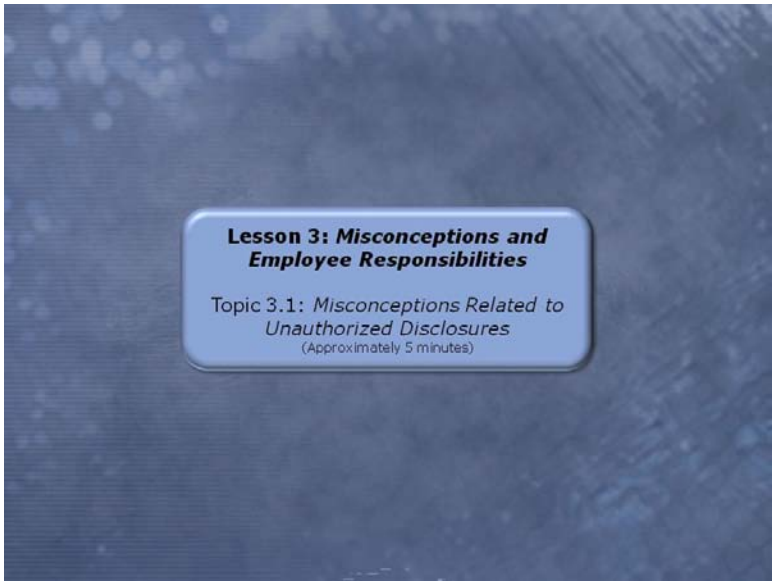
Lesson 2: Summary

Throughout history, unauthorized disclosures have caused significant damage to our national security. Media leaks can be associated with six categories of damage, which can also be applied to other unauthorized disclosures, including:

- Potential Loss of Life
- Damage to Sources and Methods
- Effect on International Alliances
- Financial Costs
- Impact to Foreign Policy
- Misinforming or Distorting Public Perception

It is essential that you are aware of the impact that unauthorized disclosures can have on the ability of the IC to provide timely and actionable intelligence in support of national security objectives.

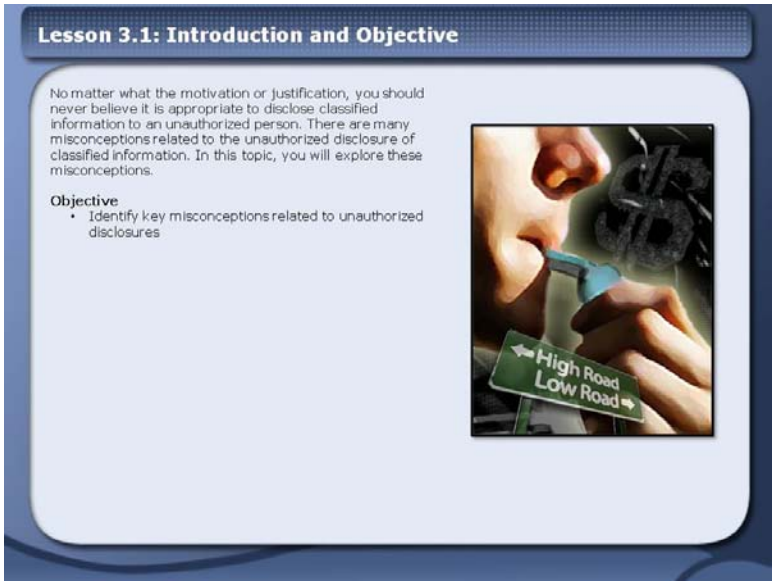
(Image Alt: Collage of a newspaper headline, money, the Soviet hammer and sickle, and a Soviet limousine.)



Lesson 3: Misconceptions and Employee Responsibilities

Topic 3.1: Misconceptions Related to Unauthorized Disclosures

(Approximately 5 minutes)

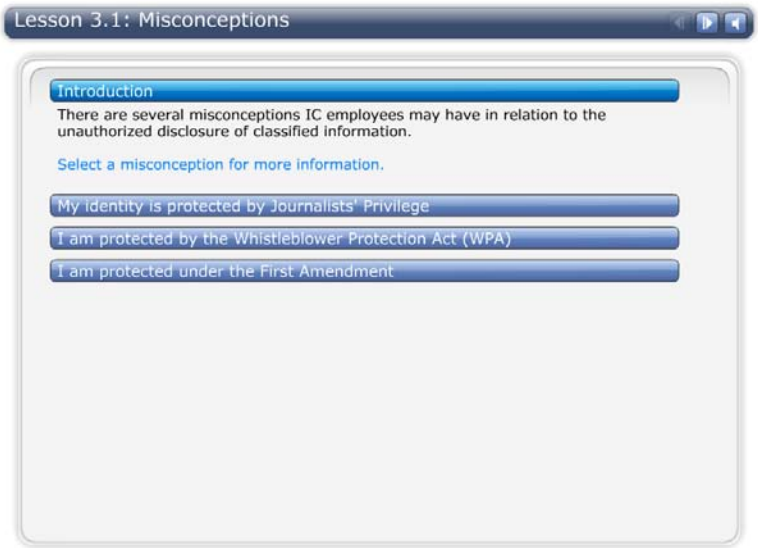


Lesson 3.1: Introduction and Objective
No matter what the motivation or justification, you should never believe it is appropriate to disclose classified information to an unauthorized person. There are many misconceptions related to the unauthorized disclosure of classified information. In this topic, you will explore these misconceptions.

Objective

- Identify key misconceptions related to unauthorized disclosures

(Image Alt: Collage of a person blowing a whistle, a dollar symbol, and a road sign with arrows pointing to “High Road” and “Low Road.”)



Lesson 3.1: Misconceptions
Introduction
There are several misconceptions IC employees may have in relation to the unauthorized disclosure of classified information.

Select a misconception for more information.

My identity is protected by Journalists' Privilege
Misconception: Journalists' Privilege allows a reporter to withhold the identity of a government source during grand jury proceedings.

Truth: Though a journalist may tell a potential government source that the source's identity is safe as a way to motivate the source to disclose information, there is no federal privilege that allows a journalist to protect the identity of a source during grand jury proceedings.

Quote:
"Reporters, like other citizens, [must] respond to relevant questions put to them in the course of a valid grand jury investigation or criminal trial."

~*Branzburg vs. Hayes* (1972)

According to the Justice Department, journalists have been subpoenaed on 19 occasions between 1991 and 2007. In once recent incident, journalist Judith Miller was imprisoned for 85 days for contempt of court prior to ultimately identifying her government source.

(Image Alt: Judith Miller behind bars.)

I am protected by the Whistleblower Protection Act (WPA)
Misconception: Unauthorized disclosures are protected by the *WPA* of 1989 and the *IC WPA* of 1998.

Truth: The *WPA* and *IC WPA* do authorize the disclosure of classified information, but it must be in the proper venue and only to authorized individuals such as an agency Inspector General, specific members

of Congress, or other authorized government officials as delineated in these statutes. The media is NOT an authorized recipient of classified information under either of these laws.

The intent of the *WPA* is to protect "whistleblowers" from any adverse actions an agency makes in retaliation for whistleblowing activity such as reporting a violation of a law, rule, or regulation; gross mismanagement; gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety. It does not protect “whistleblowers” from adverse actions taken for any other conduct, and it does not protect leakers who make unauthorized disclosures.

(Image Alt: Collage of a whistle and the cover of the *Federal Whistleblower Laws and Regulations*.)

I am protected under the First Amendment
Misconception: Unauthorized disclosures are always protected as free speech under the *First Amendment of the Constitution*.

Truth: Considering published court opinions, the *First Amendment* is not guaranteed as a valid defense for a government employee who discloses classified information.

Quote:
“It would be frivolous to assert … that the *First Amendment* … confers a license on either the reporter or his news sources to violate valid criminal laws. [N]either reporter nor source is immune from conviction for such conduct …”

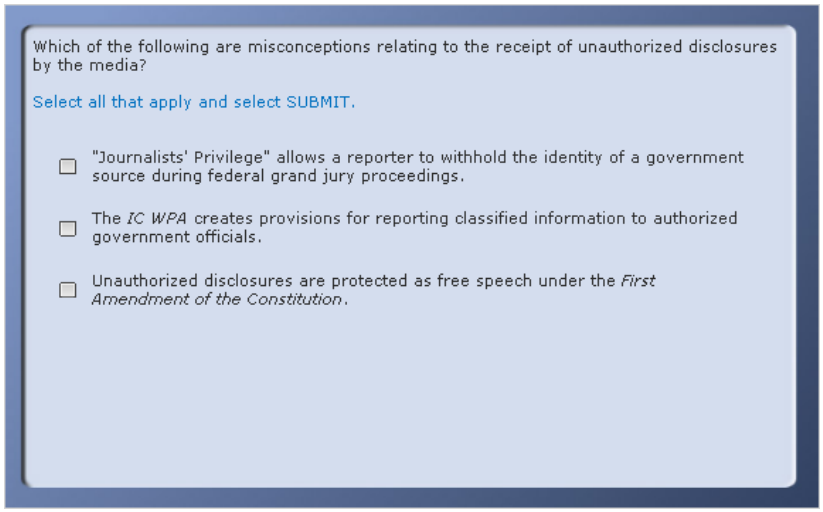
~ Supreme Court Justice Byron White, *Branzburg v. Hayes 408 U.S. 665* (1972)

Quote:
“[T]he *First Amendment* imposes no blanket prohibition on prosecution for unauthorized leaks of classified information.”

~Judge Harvie Wilkinson, *4th Circuit U.S. v Samuel Morison* (1985)

(Image Alt: Collage of a governing document, Judge Harvie Wilkinson, and Supreme Court Justice Byron White.)

Lesson 3.1: Knowledge Check



1. **Which of the following are misconceptions relating to the receipt of unauthorized disclosures by the media?**

Select all that apply and select SUBMIT.

a) "Journalists' Privilege" allows a reporter to withhold the identity of a government source during federal grand jury proceedings.
b) The *IC WPA* creates provisions for reporting classified information to authorized government officials.
c) Unauthorized disclosures are protected as free speech under the *First Amendment of the Constitution*.

Correct Responses:

a) "Journalists' Privilege" allows a reporter to withhold the identity of a government source during federal grand jury proceedings.
c) Unauthorized disclosures are protected as free speech under the *First Amendment of the Constitution*.

Feedback when correct:
That's right! You selected the correct responses.

The *IC WPA* does create provisions for reporting classified information to authorized agency officials, such as an agency Inspector General, the Department of Justice (DoJ), or specific members of Congress.

Feedback when incorrect:
You did not select the correct responses. The first and third responses are misconceptions.

Response 1: Journalists' Privilege allows a reporter to withhold the identity of a government source during grand jury proceedings.

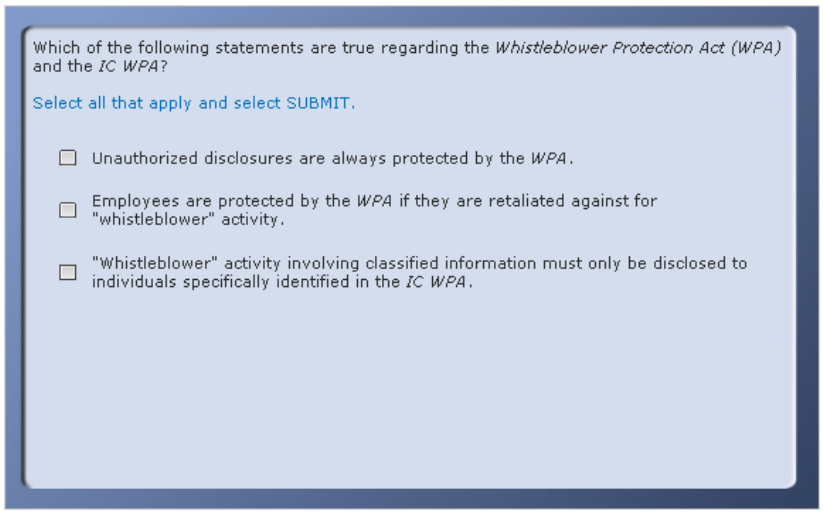
This is a misconception. Though a journalist may tell a potential government source that the source's identity is safe as motivation for the source to disclose information, there is no federal privilege that allows a journalist to protect the identity of a source during grand jury proceedings.

Response 2: The *IC WPA* creates provisions for reporting classified information to authorized government officials.

This is True. Authorized government officials include an agency Inspector General, or specific members of Congress.

Response 3: Unauthorized disclosures are protected as free speech under the *First Amendment of the Constitution*.

This is a misconception. Based on several court rulings, the *First Amendment* is not considered a valid defense for a cleared employee who discloses classified information.



2. Which of the following statements are true regarding the *Whistleblower Protection Act (WPA)* and the *IC WPA*?

Select all that apply and select SUBMIT.

a) Unauthorized disclosures are always protected by the *WPA*.
b) Employees are protected by the *WPA* if they are retaliated against for "whistleblower" activity.
c) "Whistleblower" activity involving classified information must only be disclosed to individuals specifically identified in the *IC WPA*.

Correct Responses:

b) Employees are protected by the *WPA* if they are retaliated against for "whistleblower" activity.
c) "Whistleblower" activity involving classified information must only be disclosed to individuals specifically identified in the *IC WPA*.

Feedback when correct:
That's right! You selected the correct responses.

Feedback when incorrect:
You did not select the correct responses. The second and third responses are correct.

Response 1: Unauthorized disclosures are always protected by the *WPA*.

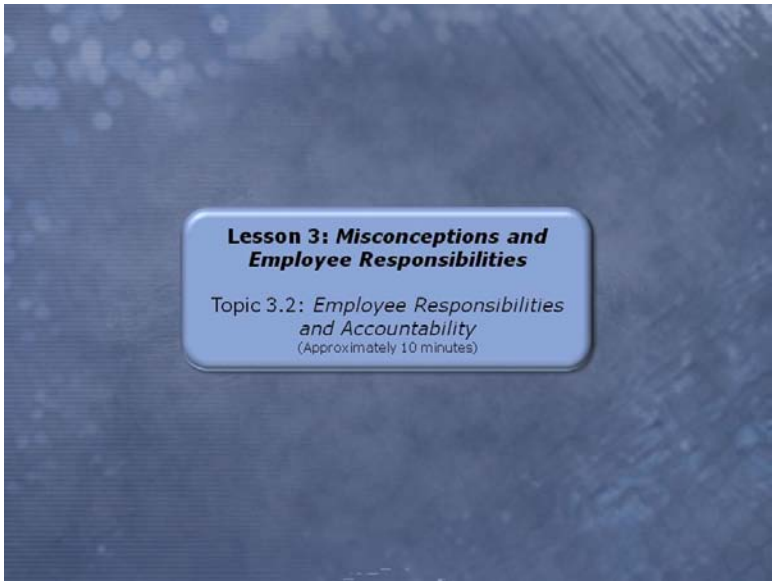
This is not true. Unauthorized disclosures are never protected by the *WPA*. Disclosures to authorized individuals under the *IC WPA* are not unauthorized disclosures. The *IC WPA* does identify proper venues for the disclosure of classified information to authorized individuals such as authorized agency officials, an agency Inspector General, or specific members of Congress; the media is not recognized as an authorized recipient of classified information. Therefore, unauthorized disclosure to the media is not protected by the *WPA*.

Response 2: Employees are protected by the *WPA* if they are retaliated against for "whistleblower" activity.

This is true. The intent of the *WPA* is to protect "whistleblowers" from any adverse actions an agency makes in retaliation for "whistleblower" activity such as reporting a violation of a law, rule, or regulation; gross mismanagement; gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety. It does not protect "whistleblowers" from adverse actions taken for any other conduct, nor does it protect individuals who make unauthorized disclosures.

Response 3: "Whistleblower" activity involving classified information must only be disclosed to individuals specifically identified in the *IC WPA*.

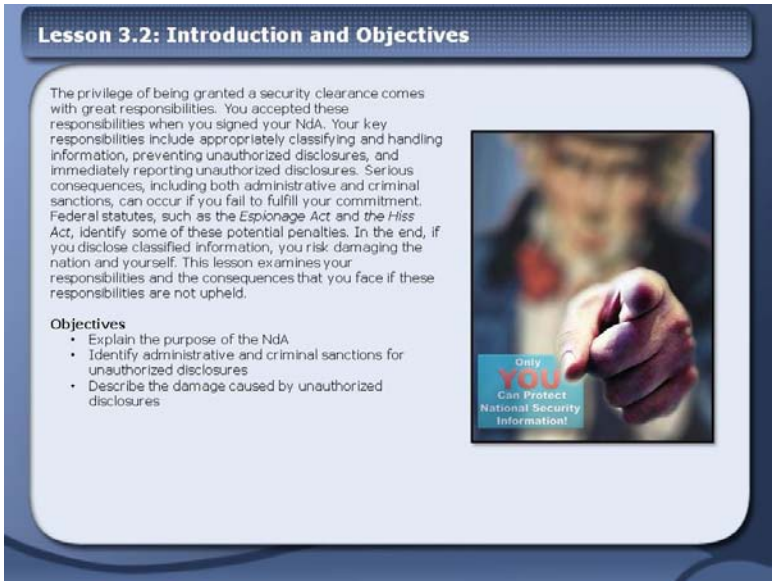
This is true. Authorized agency officials include an agency Inspector General, or specific members of Congress.



Lesson 3: Misconceptions and Employee Responsibilities

Topic 3.2: Employee Responsibilities and Accountability

(Approximately 10 minutes)



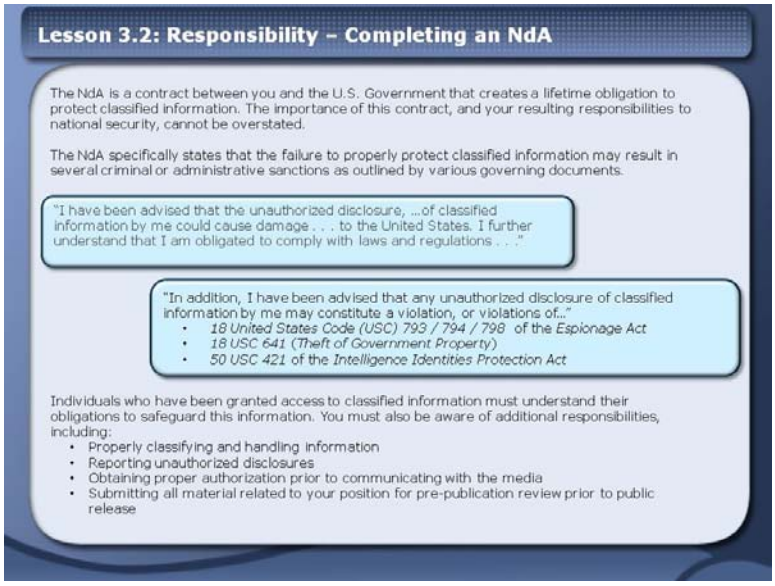
Lesson 3.2: Introduction and Objectives

The privilege of being granted a security clearance comes with great responsibilities. You accepted these responsibilities when you signed your NdA. Your key responsibilities include appropriately classifying and handling information, preventing unauthorized disclosures, and immediately reporting unauthorized disclosures. Serious consequences, including both administrative and criminal sanctions, can occur if you fail to fulfill your commitment. Federal statutes, such as the *Espionage Act* and *the Hiss Act*, identify some of these potential penalties. In the end, if you disclose classified information, you risk damaging the nation and yourself. This lesson examines your responsibilities and the consequences that you face if these responsibilities are not upheld.

Objectives

- Explain the purpose of the NdA
- Identify administrative and criminal sanctions for unauthorized disclosures
- Describe the damage caused by unauthorized disclosures

(Image Alt: Uncle Sam pointing at learner.)



Lesson 3.2: Responsibility – Completing an NdA
The NdA is a contract between you and the U.S. Government that creates a lifetime contractual obligation to protect classified information. The importance of this contract, and your resulting responsibilities to national security, cannot be overstated.

The NdA specifically indicates that the failure to properly protect classified information may result in several criminal or administrative sanctions as outlined by various governing documents.

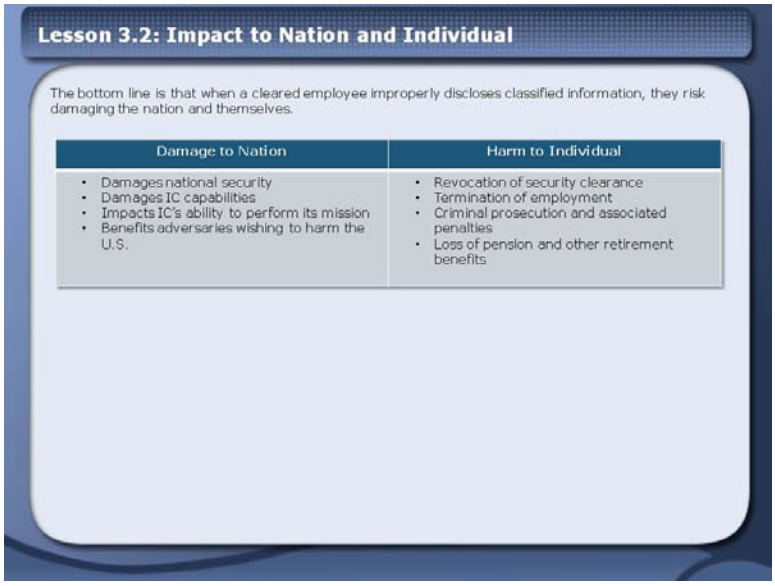
Call Out Box:
"I have been advised that the unauthorized disclosure, …of classified information by me could cause damage…to the United States. I further understand that I am obligated to comply with laws and regulations…"

Call Out Box:
"In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations of…"

- *18 United States Code (USC) 793 / 794 / 798* of the *Espionage Act*
- *18 USC 641* (*Theft of Government Property*)
- *50 USC 421* of *the Intelligence Identities Protection Act*

Individuals who have been granted access to classified information must understand their obligations to safeguard classified information. You must also be aware of additional responsibilities, including:

- Properly classifying and handling information
- Reporting unauthorized disclosures
- Obtaining proper authorization prior to communicating with the media
- Submitting all material related to your position for pre-publication review prior to public release



Lesson 3.2: Administrative and Criminal Sanctions
The type of sanction which can be levied depends on the nature and severity of the disclosure.

Administrative
Administrative sanctions include:

- Suspension without pay
- Revocation of clearance
- Termination of employment

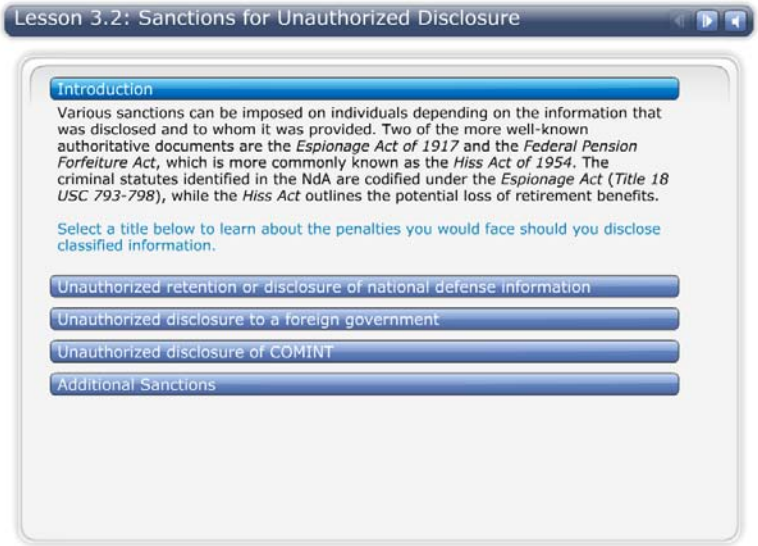
Federal statute specifically allows the heads of agencies to terminate an employee if they believe the termination is necessary in the interest of national security.

Criminal
Criminal sanctions include:

- Incarceration
- Fines
- Death penalty (under very specific circumstances)

Several of the criminal statutes identified on the NdA are part of the 1917 *Espionage Act*.

(Image Alt: Collage of man looking through prison bars, a contract being ripped in half, and an employee packing up his desk.)



Lesson 3.2: Sanctions for Unauthorized Disclosure

Introduction

Various sanctions can be imposed on individuals depending on the information that was disclosed and to whom it was provided. Two of the more well-known authoritative documents are the *Espionage Act of 1917* and the *Federal Pension Forfeiture Act*, which is more commonly known as the *Hiss Act of 1954*. The criminal statutes identified in the NdA, are codified under the *Espionage Act* (*Title 18 USC 793-798*), while the *Hiss Act* outlines the potential loss of retirement benefits.

Select a title below to learn about the penalties you would face should you disclose classified information.

Unauthorized retention or disclosure of national defense information

Section 793 of the *Espionage Act* discusses the unauthorized retention or disclosure of national defense information to any person not entitled to receive it. If you improperly disclose or retain national defense information you can be fined, incarcerated for up to ten years, or both.

Unauthorized disclosure to a foreign government

The *Espionage Act of 1917* is best recognized for *Section 794* which prohibits the disclosure of classified information to a foreign government. If you disclose classified information to a foreign government, you can be punished by death or incarcerated for any term of years up to life.

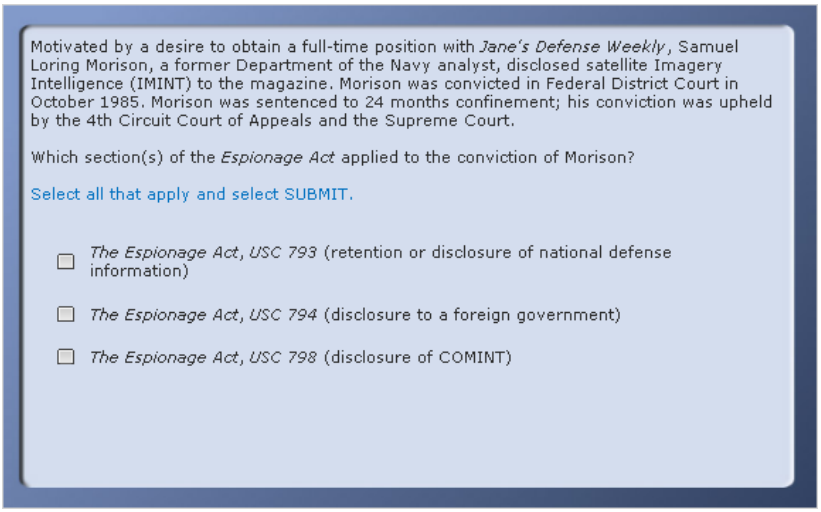
Unauthorized disclosure of COMINT

Section 798 of the *Espionage Act* specifically prohibits the disclosure or publication of communications intelligence (COMINT) to any unauthorized person. If you improperly disclose COMINT, you can be fined, incarcerated for up to ten years, or both.

Additional Sanctions

In accordance with the *Hiss Act* which was passed in 1954 and amended in 1961, an individual convicted of certain offenses, including the provisions of the *Espionage Act*, may not be paid a federal annuity or pension.

Lesson 3.2: Knowledge Check 1



1. **Motivated by a desire to obtain a full-time position with *Jane's Defense Weekly*, Samuel Loring Morison, a former Department of the Navy analyst, disclosed satellite Imagery Intelligence (IMINT) to the magazine. Morison was convicted in Federal District Court in October 1985. Morison was sentenced to 24 months confinement; his conviction was upheld by the 4th Circuit Court of Appeals and the Supreme Court.**

Which section(s) of the Espionage Act applied to the conviction of Morison?

Select all that apply and select SUBMIT.

a) *The Espionage Act*, *USC 793* (retention or disclosure of national defense information)
b) *The Espionage Act*, *USC 794* (disclosure to a foreign government)
c) *The Espionage Act*, *USC 798* (disclosure of COMINT)

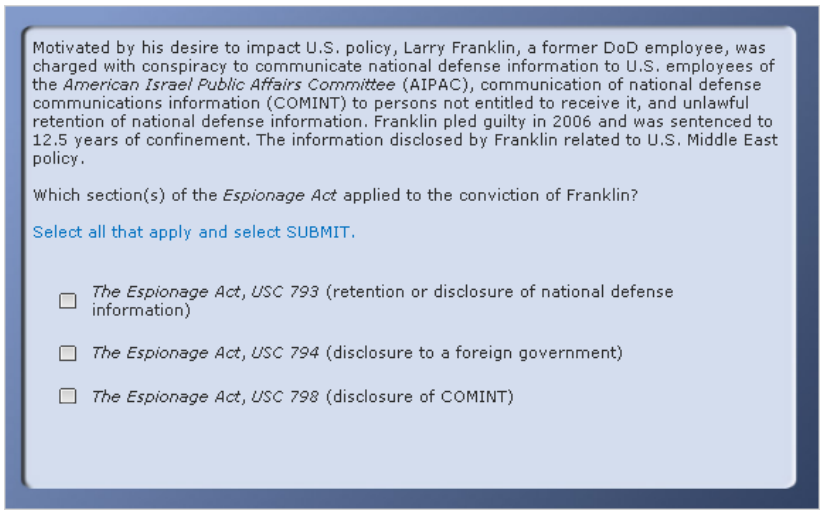
Correct Response:

a) *The Espionage Act*, *USC 793* (retention or disclosure of national defense information)

Feedback when correct:
That's right! You selected the correct response.

Feedback when incorrect:
You did not select the correct response.

The correct response is *The Espionage Act*, *USC 793*. *USC 794* is not correct because there was no foreign entity involved. *USC 798* is not correct because the disclosed information was IMINT rather than COMINT.



2. **Motivated by his desire to impact U.S. policy, Larry Franklin, a former DoD employee, was charged with conspiracy to communicate national defense information to U.S. employees of the American Israel Public Affairs Committee (AIPAC), communication of national defense communications information (COMINT) to persons not entitled to receive it, and unlawful retention of national defense information. Franklin pled guilty in 2006 and was sentenced to 12.5 years of confinement. The information disclosed by Franklin related to U.S. Middle East policy.**

Which section(s) of the Espionage Act applied to the conviction of Franklin?

Select all that apply and select SUBMIT.

a) *The Espionage Act*, *USC 793* (retention or disclosure of national defense information)
b) *The Espionage Act*, *USC 794* (disclosure to a foreign government)
c) *The Espionage Act*, *USC 798* (disclosure of COMINT)

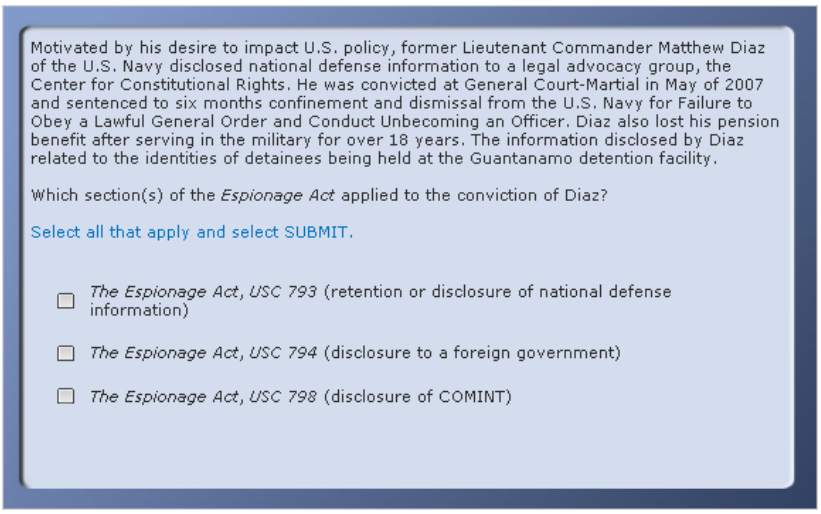
Correct Responses:

a) *The Espionage Act*, *USC 793* (retention or disclosure of national defense information)
c) *The Espionage Act*, *USC 798* (disclosure of COMINT)

Feedback when correct:
That's right! You selected the correct responses.

Feedback when incorrect:
You did not select the correct responses.

The correct responses are *The Espionage Act*, *USC 793* (retention or disclosure of national defense information) and *The Espionage Act*, *USC 798* (disclosure of COMINT). *USC 794* is not correct because there was not a foreign entity involved.



3. **Motivated by his desire to impact U.S. policy, former Lieutenant Commander Matthew Diaz of the U.S. Navy disclosed national defense information to a legal advocacy group, the Center for Constitutional Rights. He was convicted at General Court-Martial in May of 2007 and sentenced to six months confinement and dismissal from the U.S. Navy for Failure to Obey a Lawful General Order and Conduct Unbecoming an Officer. Diaz also lost his pension benefit after serving in the military for over 18 years. The information disclosed by Diaz related to the identities of detainees being held at the Guantanamo detention facility.**

Which section(s) of the Espionage Act applied to the conviction of Diaz?

Select all that apply and select SUBMIT.

a) *The Espionage Act*, *USC 793* (retention or disclosure of national defense information)
b) *The Espionage Act*, *USC 794* (disclosure to a foreign government)
c) *The Espionage Act*, *USC 798* (disclosure of COMINT)

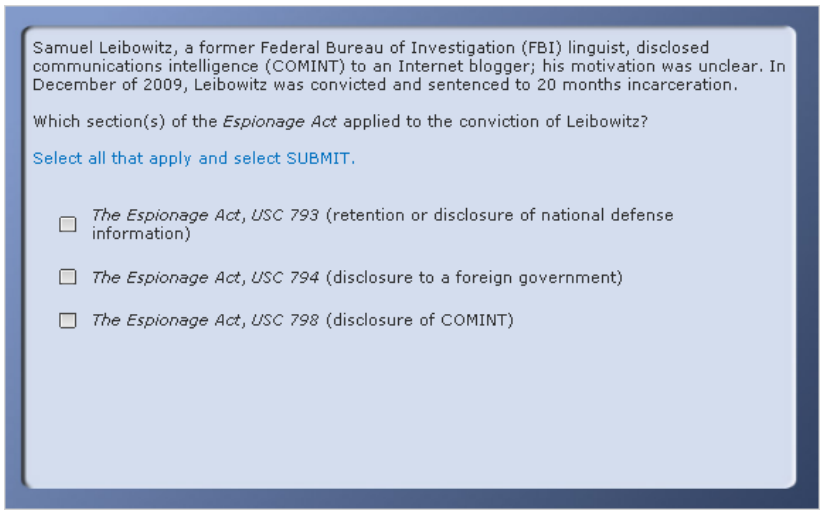
Correct Response:

a) *The Espionage Act*, *USC 793* (retention or disclosure of national defense information)

Feedback when correct:
That's right! You selected the correct response.

Feedback when incorrect:
You did not select the correct response.

The correct response is *The Espionage Act*, *USC 793* (retention or disclosure of national defense information). *USC 794* is not correct because there was no foreign entity involved and *USC 798* is not correct because the information was not COMINT.



4. Samuel Leibowitz, a former Federal Bureau of Investigation (FBI) linguist, disclosed communications intelligence (COMINT) to an Internet blogger; his motivation was unclear. In December of 2009, Leibowitz was convicted and sentenced to 20 months incarceration.

Which section(s) of the *Espionage Act* applied to the conviction of Leibowitz?

Select all that apply and select SUBMIT.

a) *The Espionage Act*, *USC 793* (retention or disclosure of national defense information)
b) *The Espionage Act*, *USC 794* (disclosure to a foreign government)
c) *The Espionage Act*, *USC 798* (disclosure of COMINT)

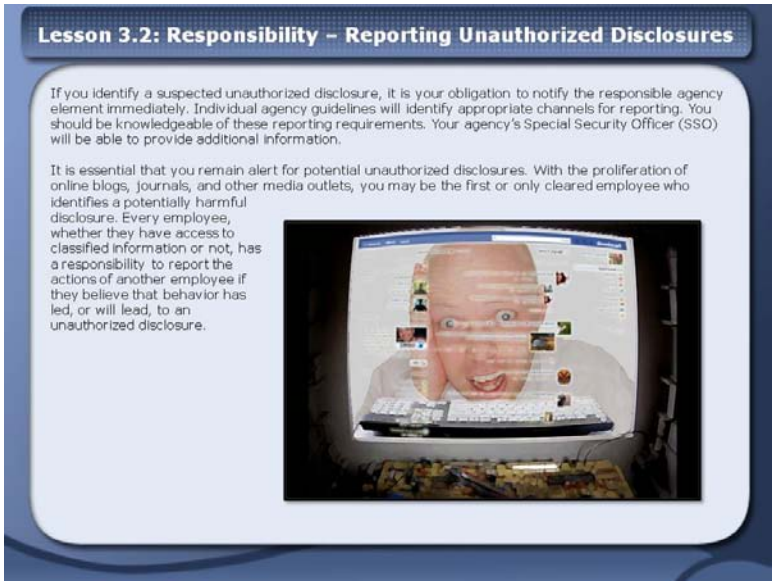
Correct Response:

c) *The Espionage Act*, *USC 798* (disclosure of COMINT)

Feedback when correct:
That's right! You selected the correct response.

Feedback when incorrect:
You did not select the correct response.

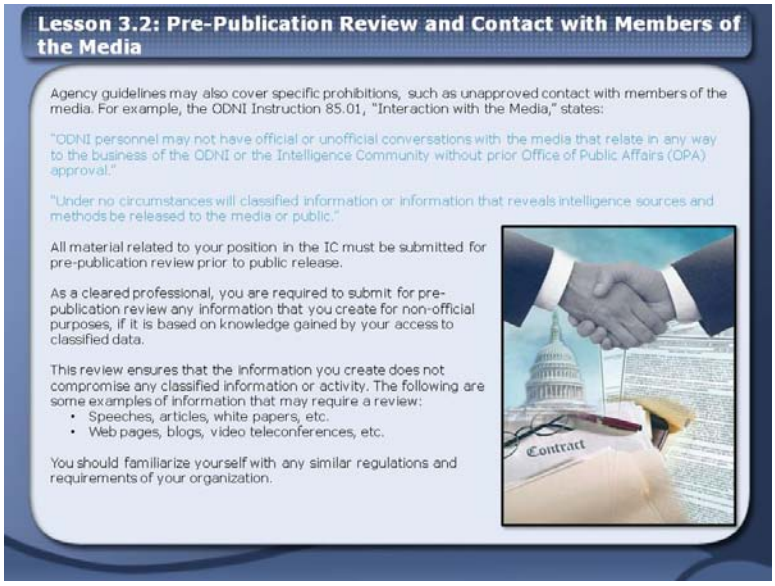
The correct response is *The Espionage Act*, *USC 798* (disclosure of COMINT). *USC 793* is not the best response because the intelligence disclosed was COMINT, which is specifically covered in *USC 798*. *USC 794* is not correct because there was not a foreign entity involved.



Lesson 3.2: Responsibility – Reporting Unauthorized Disclosures
If you identify a suspected unauthorized disclosure, it is your obligation to notify the responsible agency element immediately. Individual agency guidelines will identify appropriate channels for reporting. You should be knowledgeable of these reporting requirements. Your agency's Special Security Officer (SSO) will be able to provide additional information.

It is essential that you remain alert for potential unauthorized disclosures. With the proliferation of online blogs, journals, and other media outlets, you may be the first or only cleared employee who identifies a potentially harmful disclosure. Every employee, whether they have access to classified information or not, has a responsibility to report the actions of another employee if they believe that behavior has led, or will lead, to an unauthorized disclosure.

(Image Alt: A shocked man looking at a social networking site.)



Lesson 3.2: Pre-Publication Review and Contact with Members of the Media
Agency guidelines may also cover specific prohibitions, such as unapproved contact with members of the media. For example, the Office of the Director of National Intelligence (ODNI) Instruction 85.01, "Interaction with the Media," states:

Quote:
"ODNI personnel may not have official or unofficial conversations with the media that relate in any way to the business of the ODNI or the Intelligence Community without prior Office of Public Affairs (OPA) approval."

Quote:
"Under no circumstances will classified information or information that reveals intelligence sources and methods be released to the media or public."

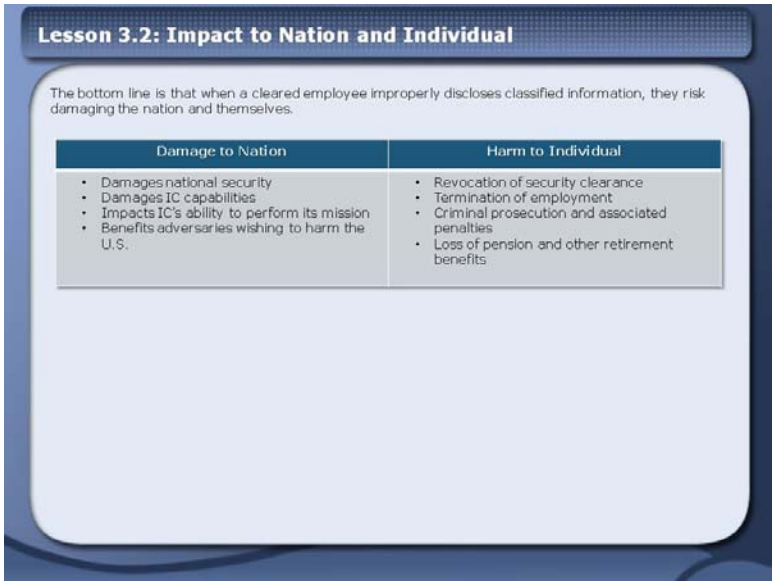
All material related to your position in the IC must be submitted for pre-publication review prior to public release.

As a cleared professional, you are required to submit for pre-publication review any information that you create for non-official purposes, if it is based on knowledge gained by your access to classified data. This review ensures that the information you create does not compromise any classified information or activity. The following are some examples of information that may require a review:

- Speeches, articles, white papers, etc.
- Web pages, blogs, video teleconferences, etc.

You should familiarize yourself with any similar regulations and requirements of your organization.

(Image Alt: Collage of a handshake, governing documents, the Capitol, and eyeglasses and a pen on a contract.)



Lesson 3.2: Impact to Nation and Individual
The bottom line is that when a cleared employee improperly discloses classified information, they risk damaging the nation and themselves.

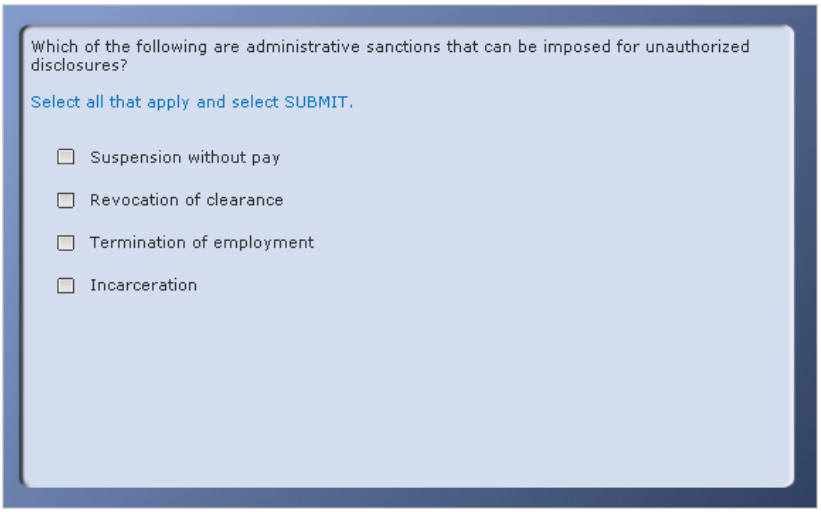
Damage to Nation

- Damage to national security
- Damage to IC capabilities
- Impact IC's ability to perform its mission
- Benefit adversaries wishing to harm the U.S.

Harm to Individual

- Revocation of security clearance
- Termination of employment
- Criminal prosecution and associated penalties
- Loss of pension and other retirement benefits

Lesson 3.2: Knowledge Check 2



1. Which of the following are administrative sanctions that can be imposed for unauthorized disclosures?

Select all that apply and select SUBMIT.

a) Suspension without pay
b) Revocation of clearance
c) Termination of employment
d) Incarceration

Correct Responses:

a) Suspension without pay
b) Revocation of clearance
c) Termination of employment

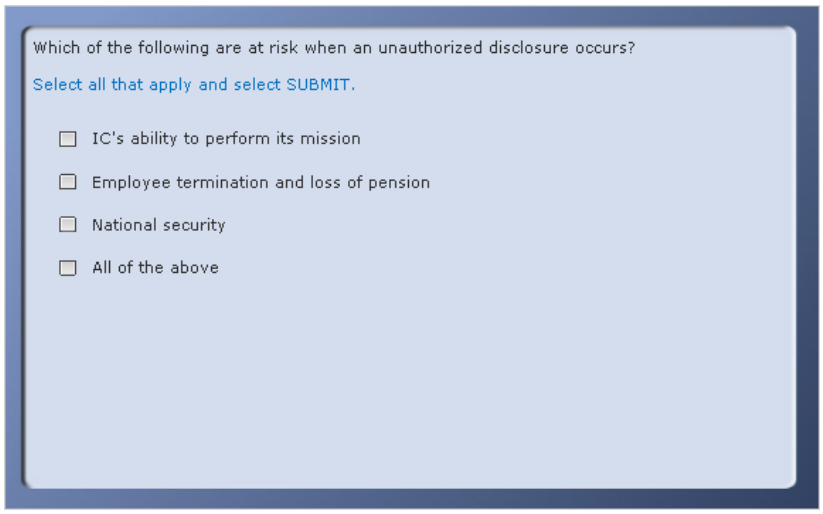
Feedback when correct:
That's right! You selected the correct responses.

Feedback when incorrect:
You did not select the correct responses.

The correct responses are:

- Suspension without pay
- Revocation of clearance
- Termination of employment

Incarceration is a criminal sanction, which could apply for making an unauthorized disclosure.



2. Which of the following are at risk when an unauthorized disclosure occurs?

a) IC's ability to perform its mission
b) Employee termination and loss of pension
c) National security
d) All of the above

Correct Response:

d) All of the above

Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.
The correct response is: “All of the above. “

Potential damage to the nation includes:

- Impact to IC’s ability to perform its mission
- Damage to national security

As well as:

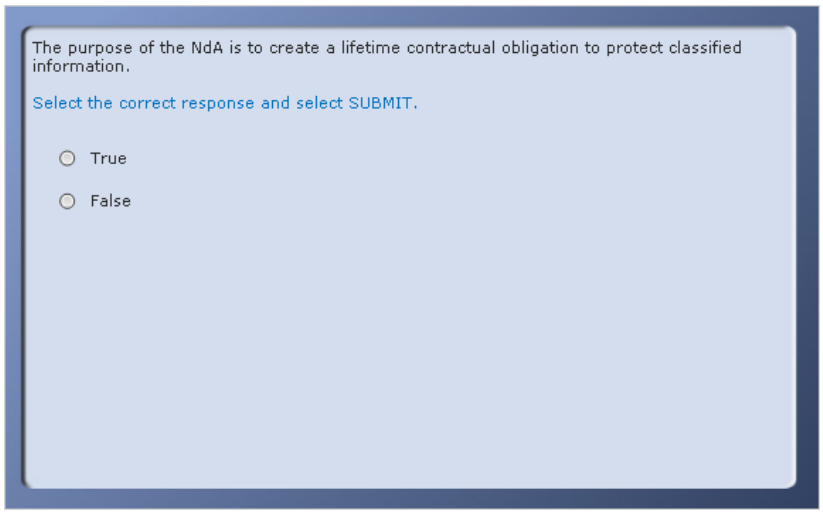
- Damage to IC’s capabilities
- Benefit to adversaries wishing to harm the U.S.

Potential damage to the IC employee includes:

- Termination of employment

As well as:

- Revocation of security clearance
- Criminal prosecution and associated penalties
- Loss of pension and other retirement benefits



3. The purpose of the NdA is to create a lifetime contractual obligation to protect classified information.

a) True
b) False

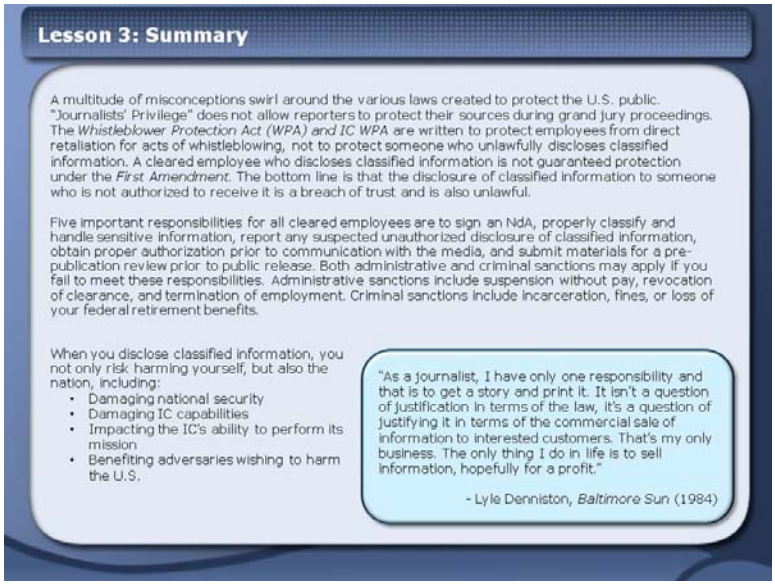
Correct Response:
True

Feedback when correct:
That's right! You selected the correct response.

The NdA creates a lifetime contractual obligation to protect classified information. The NdA specifically indicates that the failure to properly protect classified information may result in several criminal or administrative sanctions.

Feedback when incorrect:
You did not select the correct response. The correct response is True.

The NdA creates a lifetime contractual obligation to protect classified information. It specifically indicates that the failure to properly protect classified information may result in several criminal or administrative sanctions.



Lesson 3: Summary

A multitude of misconceptions swirl around the various laws created to protect the U.S. public. "Journalistic Privilege" does not allow reporters to protect their sources during grand jury proceedings. The *Whistleblower Protection Act (WPA) and IC WPA* are written to protect employees from direct retaliation for acts of whistleblowing, not to protect someone who unlawfully discloses classified information. A cleared employee who discloses classified information is not guaranteed protection under the *First Amendment.* The bottom line is that the disclosure of classified information to someone who is not authorized to receive it is a breach of trust and is also unlawful.

Five important responsibilities for all cleared employees are to sign an NdA, properly classify and handle sensitive information, report any suspected unauthorized disclosure of classified information, obtain proper authorization prior to communication with the media, and submit materials for a pre-publication review prior to public release. Both administrative and criminal sanctions may apply if you fail to meet these responsibilities. Administrative sanctions include suspension without pay, revocation of clearance, and termination of employment. Criminal sanctions include incarceration, fines, or loss of your federal retirement benefits.

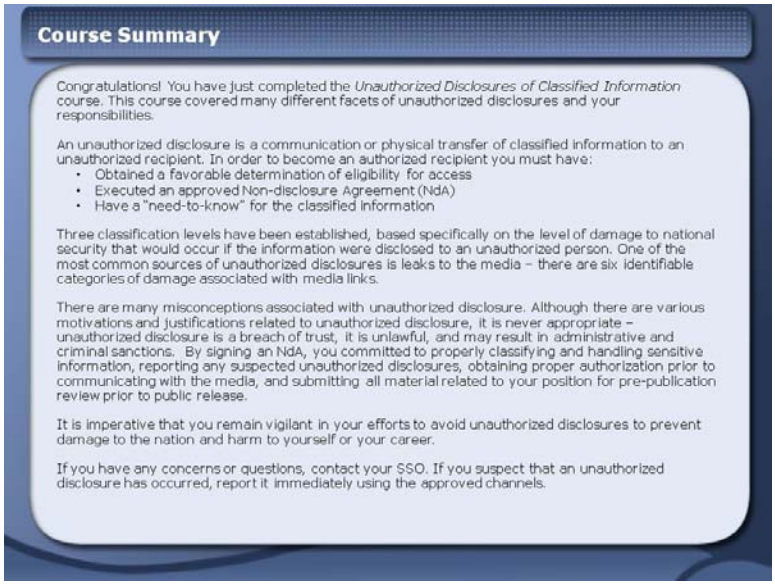
When you disclose classified information, you not only risk harming yourself, but also the nation, including:

- Damaging national security
- Damaging IC capabilities
- Impacting the IC's ability to perform its mission
- Benefiting adversaries wishing to harm the U.S.

Call Out Box:

"As a journalist, I have only one responsibility and that is to get a story and print it. It isn't a question of justification in terms of the law, it's a question of justifying it in terms of the commercial sale of information to interested customers. That's my only business. The only thing I do in life is to sell information, hopefully for a profit."

~Lyle Denniston, *Baltimore Sun* (1984)



Course Summary

Congratulations! You have just completed the *Unauthorized Disclosures of Classified Information* course. This course covered many different facets of unauthorized disclosures and your responsibilities.

An unauthorized disclosure is a communication or physical transfer of classified information to an unauthorized recipient. In order to become an authorized recipient you must have:

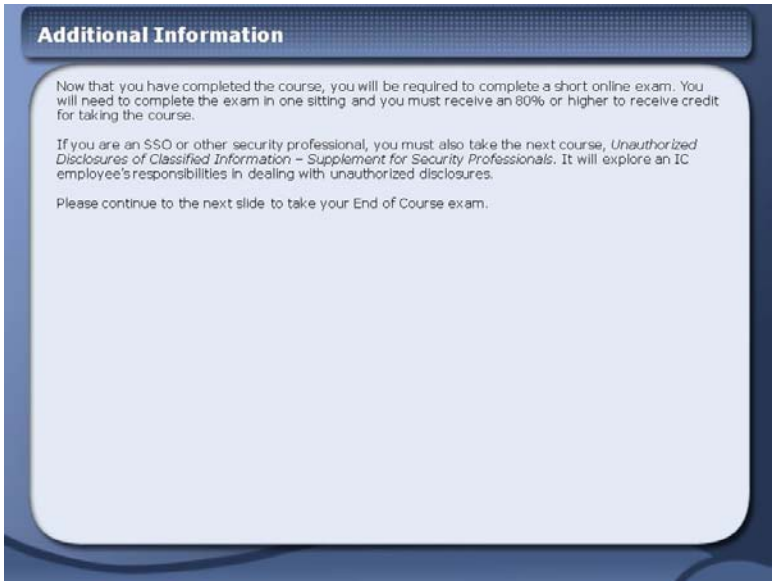
- Obtained a favorable determination of eligibility for access
- Executed an approved Non-disclosure Agreement (NdA)
- Have a "need-to-know" for the classified information

Three classification levels have been established, based specifically on the level of damage to national security that would occur if the information were disclosed to an unauthorized person. One of the most common sources of unauthorized disclosures is leaks to the media – there are six identifiable categories of damage associated with media links.

There are many misconceptions associated with unauthorized disclosure. Although there are various motivations and justifications related to unauthorized disclosure, it is never appropriate – unauthorized disclosure is a breach of trust, it is unlawful, and may result in administrative and criminal sanctions. By signing an NdA, you committed to properly classifying and handling sensitive information, reporting any suspected unauthorized disclosures, obtaining proper authorization prior to communicating with the media, and submitting all material related to your position for pre-publication review prior to public release.

It is imperative that you remain vigilant in your efforts to avoid unauthorized disclosures to prevent damage to the nation and harm to yourself or your career.

If you have any concerns or questions, contact your SSO. If you suspect that an unauthorized disclosure has occurred, report it immediately using the approved channels.



Additional Information

Now that you have completed the course, you will be required to complete a short online exam. You will need to complete the exam in one sitting and you must receive an 80% or higher to receive credit for taking the course.

If you are an SSO or other security professional, you must also take the next course, *Unauthorized Disclosures of Classified Information – Supplement for Security Professionals*. It will explore an IC employee's responsibilities in dealing with unauthorized disclosures.

Please continue to the next slide to take your End of Course exam.