Student Guide

Course: NISP Reporting Requirements

Lesson 1: Course Introduction

Course Information

Purpose	Provide a thorough understanding of the National Industrial Security Program (NISP) reporting requirements, including why to report, what to report, and how to report on various types of events and information
Audience	• Facility security officers (FSOs) at cleared DoD contractor facilities participating in the NISP • Other contractor security personnel • DSS Industrial Security Representatives (IS Reps) • DoD Industrial Security Specialists
Pass/Fail %	75% on final examination
Estimated completion time	75 minutes

Course Overview

The National Industrial Security Program, or NISP, is a government-industry partnership that was forged to help protect our national security. Successful implementation of the NISP requires effective communication between government and industry. One way that the government communicates with industry is by issuing directives and guidance. Likewise, one way that industry communicates with the government is by submitting reports. Representing industry, the facility security officer, or FSO, is a key player in this program, serving as the communication link between industry and the government.

In this course, you will explore the FSO's role in reporting to the government. You will learn about the structure of the NISP as it relates to reporting. And finally, you will learn why reporting is required, what must be reported, and how certain information is to be reported.

Course Objectives

Here are the course objectives:

- Identify the importance of reporting and the potential effects that failure to report can have on national security and the warfighter
- Identify the legal and regulatory basis for NISP reporting requirements
- Identify the circumstances requiring reporting that—
    - Affect the status of the personnel security clearance (PCL), including attempts by suspicious contacts to compromise a cleared employee
    - Affect the status of the facility security clearance (FCL), including attempts by suspicious contacts to gain access to classified information
    - Affect the proper safeguarding of classified information
    - Indicate that classified information may have been lost or compromised
- Identify the reports that are required by the NISPOM
- Identify the reporting process for each type of information

Course Structure

This course is organized into the lessons listed here:

- Course Introduction
- Understanding Reporting in the NISP
- Reporting Personnel and Facility Changes
- Reporting Security Concerns and Violations
- Course Conclusion

Student Guide

Course: NISP Reporting Requirements

Lesson 2: Understanding Reporting in the NISP

Lesson Introduction

1. Importance of Reporting

You've heard the stories of Robert Hanssen and Aldrich Ames, two civil servants who spent many years leading double lives as secret agents for Russia. But what about Chi Mak, Greg Chung, and Chi Tong Kuok? Each of these individuals spied for China and targeted a cleared contractor facility like yours. Did you know that cleared contractor facilities are attractive targets of foreign intelligence services, and that in fact, they are targeted with alarming frequency? And that each of these individuals engaged in activities that should have been reported by employees of the facilities they targeted?

Chi Mak was the center of a web of spies that included Chung, an employee of a cleared contractor facility, and Kuok, who solicited information from cleared contractor employees. When Chung was caught, the FBI discovered that he had stored 300,000 pages of classified and sensitive documents in his home. Did any of Chung's coworkers ever see him taking classified materials home or engaging in other suspicious activities? If his behavior had been reported earlier, then it might have been possible to prevent a significant loss of classified information. Kuok's arrest came as the result of a suspicious contact report made to DSS by a cleared contractor whose conscientious reporting thus forestalled the loss of highly sensitive cryptographic communications technology and export-controlled information and potentially saved lives.

Why do contractors need to be concerned with reporting? To protect our national security, to protect our warfighters, to protect our economic stability, and to protect your company's own competitive advantage in the marketplace.

2. Objectives

Before you learn the specifics of how and what a facility security officer, or FSO, is to report, it is important to understand why reporting is an integral part of the FSO's responsibilities. Here are the lesson objectives:

- Identify the importance of reporting and the potential effects that failure to report can have on national security and the warfighter
- Identify the legal and regulatory basis for NISP reporting requirements

- Identify the circumstances requiring reporting that—
    - Affect the status of the facility security clearance (FCL), including attempts by suspicious contacts to gain access to classified information
    - Affect the status of the personnel security clearance (PCL), including attempts by suspicious contacts to compromise a cleared employee
    - Affect the proper safeguarding of classified information
    - Indicate that classified information may have been lost or compromised

Reporting Requirements

1. Why You Must Report

Why must you report? You work with cleared personnel in a cleared facility, so what is there to report? As it turns out, there is plenty. The National Industrial Security Program, or NISP, was established by Executive Order 12829. As a partnership between the U.S. government and private industry, the NISP ensures the proper protection of classified information that has been released to industry. When your company signed the DoD Security Agreement, or DD Form 441, it agreed to maintain security controls and procedures in accordance with DoD 5220.22-M, which is more commonly known as the National Industrial Security Program Operating Manual, or NISPOM.

The NISPOM establishes the baseline security procedures and requirements to ensure that safeguards employed by contractors are adequate for the protection of classified information. One such requirement, defined in NISPOM paragraph 1-300, states that contractors must report various types of information or events to the appropriate government agencies. This requirement to report applies to certain events that—

- Affect a contractor’s facility security clearance
- Affect an employee’s personnel security clearance
- Affect the proper safeguarding of classified information
- Indicate that classified information has been lost or compromised

One type of report that is of particular importance is that of suspicious contacts.

As a cleared contractor in the NISP, your company agrees to meet all applicable NISP requirements as set forth by the NISPOM, including the requirements to report. But ultimately, as your company's FSO, the responsibility to report these events belongs to you!

2. What You Must Report

The NISPOM defines various events that must be reported. These events can be separated into three broad categories.

1. Changes in personnel information are changes that could affect the personnel security clearance, or PCL, of any of a company's employees. Such changes could be related to adverse information or changes in an employee's personal status (such as death, termination, or a name change).

2. Changes in facility information are changes that could affect a contractor's facility security clearance, or FCL, including the facility's ability to protect classified information. Changes in facility information could be related to a change in physical location, a change in ownership, or a change in the company's key management personnel, or KMPs.

3. Finally, security concerns and violations are those events that show a failure to comply with the policies and procedures established by the NISPOM. Such events could result in potentially grave threats to national security or the loss or compromise of classified information. Security concerns include those events involving actual or suspected espionage, sabotage, terrorism, and subversive activities. Security violations include leaving a safe containing classified information open and unattended, removing classified information from the facility without permission, or using an unaccredited computer to process classified information.

Specific circumstances of each of these reporting categories will be discussed in greater detail throughout this course.

Reporting Methods

1. Structure of the NISP

To best understand how to perform the FSO reporting function, it is necessary to first understand the overall structure of the NISP. Recall that the NISP is a partnership between government and industry.

On the government side, the cognizant security agency, or CSA, is responsible for the protection of classified information within its purview in the NISP, including classified information that has been entrusted to industry. The CSA may oversee the NISP, but it delegates a cognizant security office, or CSO, to administer the NISP on its behalf. Reports to the government are submitted to the CSO.

On the industry side, each cleared contractor facility must have a facility security officer, or FSO. As the communication link in the partnership between government and industry, the FSO is responsible for receiving communication from the government and implementing government directives within the contractor facility. The FSO is also responsible for communicating to the government. One way that the FSO reports to the government is by submitting reports.

For the purposes of this course, we will focus on the reporting structure and processes as they apply specifically to the DoD. When the DoD is your CSA, CSA reports are submitted to the Defense Security Service, or DSS. As the CSO, the DSS receives these reports and acts on behalf of the DoD. Therefore, the FSO reports to the DoD by submitting reports to the DSS. Depending on the type of information that is being reported, reports will be submitted to one of two entities: the Industrial Security Representative, or IS Rep, at the DSS Field Office assigned to your facility or the Personnel Security Management and Oversight of Industry, or PSMO-I.

Take a moment to review the job aid on the following page, which illustrates the structure of the NISP.

Structure of the NISP

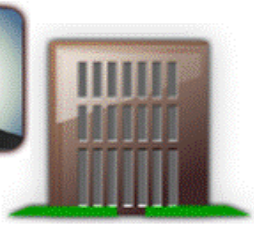
Cognizant Security Agency (CSA)
- *Oversees the NISP*

Department of Defense (DoD)

Cognizant Security Office (CSO)
- *Administers the NISP on behalf of the CSA*
- *Receives reports to the government*

Defense Security Service (DSS)

IS Rep



DSS Field Office

PSMO-I

Industrial Security Representative (IS Rep) at DSS Field Office
- *Receives reports about facility security and other issues*

Personnel Security Management and Oversight for Industry (PMSO-I)
- *Receives reports about personnel security clearances*

Facility Security Officer (FSO)
- *Receives communication from the government*
- *Implements government directives within contractor facility*
- *Submits reports to the government*

FSO

How You Must Report

A report may take a number of forms. In some cases, reporting is as simple as notifying the appropriate government entity by letter, telephone, or e-mail. In other cases, reporting may require more specific details to be supplied in a designated form.

Reports must be submitted to the CSA—in this case the DSS—but the specific entity of the DSS that you report to depends on the type of information being reported.

In general, you will submit reports on anything that might affect the personnel security clearances of any of your company's employees or anything that might affect your facility clearance or your facility's ability to protect classified materials.

Reports about personnel security clearances will be sent to the Personnel Security Management and Oversight for Industry, or PMSO-I. Reports about facility security and other issues will be sent to your IS Rep at the DSS Field Office.

In most circumstances, reports will be submitted solely to the CSA. However, in certain circumstances involving actual or suspected espionage, sabotage, terrorism, or subversive activities, reports must be submitted to the FBI, with a copy sent to DSS. In matters of national security significance, reports may also be made to a hotline, as listed in the NISPOM 1-207.

a. PSMO-I

Reports about personnel and reports affecting personnel security clearances are submitted to PSMO-I using the Joint Personnel Adjudication System, or JPAS. In most circumstances, reporting in JPAS must be done by the FSO. However, in some circumstances, information may be entered by a JPAS account manager or user.

b. DSS Field Office

Reports about your facility and its capacity to protect classified information are sent to your IS Rep at the DSS Field Office. These reports are submitted either in writing, by letter or e-mail, directly to your IS Rep or through the electronic Facility Security Clearance, or e-FCL, system.

c. FBI

Although most reports are submitted solely to DSS, some potentially grave threats to national security require immediate reporting directly to the FBI. Such threats include any information involving actual or suspected espionage, sabotage, terrorism, or subversive activities. When reporting to the FBI, an initial

report may be made by phone, but a written report must follow. The NISPOM requires that all reports to the FBI also be filed with your IS Rep.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

CSA Hotlines (NISPOM 1-207)

Defense Hotline
The Pentagon
Washington, DC 20301-1900
(800) 424-9098

NRC Hotline
U.S. Nuclear Regulatory Commission
Office of the Inspector General
Mail Stop TSD 28
Washington, DC 20555-0001
(800) 233-3497

CIA Hotline
Office of the Inspector General
Central Intelligence Agency
Washington, DC 20505
(703) 874-2600

DOE Hotline
Department of Energy
Office of the Inspector General
1000 Independence Avenue, SW, Room 5A235
Washington, DC 20585
(202) 586-4073 or (800) 541-1625

Review Activity 1

Which of the following statements describe why reporting certain information is important? Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- ☐ Reporting suspicious contacts can lead to the capture of individuals seeking to harm national security.
- ☐ Reporting adverse information about employees of cleared contractor facilities can help to safeguard classified information.
- ☐ Failing to report an employee's failure to follow safeguarding procedures can lead to the disclosure of classified information, which may result in the loss of life of our warfighters.

Review Activity 2

Several regulatory and legal documents form the basis for the requirement to report. Each description on the left pairs with one of the documents on the right. Select the appropriate document for each statement. Check your answers in the Answer Key at the end of this Student Guide.

	E.O. 12829	**DD Form 441**	**NISPOM**
The baseline security procedures and requirements (including the requirement to report) that ensure protection of classified information by contractors	○	○	○
Established the partnership between the U.S. government and private industry that is known as the National Industrial Security Program	○	○	○
The contractual agreement in which contractors agree to maintain minimum security controls to protect classified information	○	○	○

Review Activity 3

Match each type of information requiring reporting to the name of the entity to which it must be reported. Write the matching letter in the space beside each entity. Check your answer in the Answer Key at the end of this Student Guide.

Type of Information	Entity
A. Actual or suspected espionage, sabotage, terrorism, or subversive activities	PSMO-I ____
B. Changes to personnel information	DSS Field Office ____
C. Changes to facility information	FBI ____

Answer Key

Review Activity 1

Which of the following statements describe why reporting certain information is important?

- ☒ Reporting suspicious contacts can lead to the capture of individuals seeking to harm national security.
- ☒ Reporting adverse information about employees of cleared contractor facilities can help to safeguard classified information.
- ☒ Failing to report an employee's failure to follow safeguarding procedures can lead to the disclosure of classified information, which may result in the loss of life of our warfighters.

Review Activity 2

Several regulatory and legal documents form the basis for the requirement to report. Each description on the left pairs with one of the documents on the right.

	E.O. 12829	**DD Form 441**	**NISPOM**
The baseline security procedures and requirements (including the requirement to report) that ensure protection of classified information by contractors	○	○	●
Established the partnership between the U.S. government and private industry that is known as the National Industrial Security Program	●	○	○
The contractual agreement in which contractors agree to maintain minimum security controls to protect classified information	○	●	○

Review Activity 3

Match each type of information requiring reporting to the name of the entity to which it must be reported.

Type of Information	Entity	
A. Actual or suspected espionage, sabotage, terrorism, or subversive activities	PSMO-I	B
B. Changes to personnel information	DSS Field Office	C
C. Changes to facility information	FBI	A

Student Guide

Course: NISP Reporting Requirements

Lesson 3: Reporting Personnel and Facility Changes

Lesson Introduction

1. Objectives

As the facility security officer, or FSO, you are required to report on various conditions related to both personnel and facility clearances. In this lesson, you will learn what circumstances require reporting and how each is to be reported. Here are the lesson objectives.

- Identify the circumstances requiring reporting that—
    - Affect the status of the facility security clearance (FCL), including attempts by suspicious contacts to gain access to classified information
    - Affect the status of the personnel security clearance (PCL), including attempts by suspicious contacts to compromise a cleared employee
- Identify the reports that are required by the NISPOM
- Identify the reporting process for each type of information

2. Overview of Personnel and Facility Changes

NISPOM paragraph 1-302 identifies 14 types of personnel- and facility-related information and events that must be reported to the cognizant security agency, or CSA.

For the most part, these reports are administrative in nature; however, that does not make them any less important. Reporting on personnel and facility changes, no matter how minor such changes may seem, is critical to maintaining accurate records on cleared individuals and facilities. Over time, such reports may reveal patterns that could signify a more serious potential threat or violation. Each of these events must be reported to the CSA, but whether they are reported to the Personnel Security Management and Oversight of Industry, or PSMO-I, or to the DSS Field Office depends upon what type of information is being reported.

In general, reports about personnel, including reports affecting the clearance status of key management personnel, or KMPs, are made to PSMO-I using either the incident report function or the Request to Research or Upgrade, or RRU, function in the Joint Personnel Adjudication System, or JPAS.

Reports about the facility, including any changes in the company's KMPs, are made to the Industrial Security Representative, or IS Rep, at the DSS Field Office assigned to your facility. These reports are submitted either in writing directly to the IS Rep or through the electronic facility security clearance, or e-FCL, system.

NISPOM 1-302	
1-302	**Reports to be Submitted to the CSA**
1-302a	Adverse Information
1-302b	Suspicious Contacts
1-302c	Change in Cleared Employee Status
1-302d	Citizenship by Naturalization
1-302e	Employees Desiring Not to Perform on Classified Work
1-302f	Standard Form (SF) 312
1-302g	Change Conditions Affecting the Facility Clearance
1-302h	Changes in Storage Capability
1-302i	Inability to Safeguard Classified Material
1-302j	Security Equipment Vulnerabilities
1-302k	Unauthorized Receipt of Classified Material
1-302l	Employee Information in Compromise Cases
1-302m	Disposition of Classified Material Terminated From Accountability
1-302n	Foreign Classified Contracts

Changes Affecting Personnel

1. Reporting on People

Of the 14 subparagraphs listed in NISPOM paragraph 1-302, there are six types of information or events related to personnel that may affect an individual employee’s personnel clearance. Most reports about cleared personnel are reported to PSMO-I via JPAS. The one exception is reports about suspicious contacts, which are reported to your IS Rep. Let’s look at each of these in closer detail.

2. Adverse Information

Of all the reports that an FSO is responsible for, the adverse information report is one of the most important. Adverse information refers to any behavior that might cause the DoD to question whether an individual should have access to classified information. What types of information might this include?

Quite simply, it includes any information that might cast doubt on an employee’s character or integrity, such as information about an employee’s financial situation, personal conduct, allegiance to the United States, reliance on drugs or alcohol, criminal

convictions, or any other factors that may call into question a person's judgment, reliability, or suitability to have access to classified information. All these factors are related to the DoD's Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Adjudicative Guidelines

The FSO should be familiar with the DoD's Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, because the factors that determine an employee's qualification to be granted a clearance are the same factors that determine an employee's qualification to maintain a clearance. These factors include discussion of each of the categories here:

- Allegiance to the United States
- Foreign influence
- Foreign preference
- Sexual behavior
- Personal conduct
- Financial considerations
- Alcohol consumption
- Drug involvement
- Emotional, mental, and personality disorders
- Criminal conduct
- Security violations
- Outside activities
- Misuse of information technology systems

NISPOM subparagraph 1-302a defines the NISP requirement to report adverse information. If you receive or become aware of any credible adverse information about a cleared employee, then you must report it to PSMO-I using the incident report function in JPAS. Be advised that the FSO's job is only to report adverse information. It is the government's job to make a final determination about whether to grant or continue an individual's personnel security clearance. Note that you should report only credible information. Do not report information based on rumor or innuendo.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Case Study

The case of Noshir S. Gowadia, a former engineer for Northrop Grumman, illustrates the importance of reporting adverse information. For 18 years, Gowadia contributed to the development of the B-2 stealth bomber. Retiring from Northrop Grumman in 1986, he struck out on his own, continuing to contract with the U.S. government on classified matters until his security clearance ended in 1997.

By all accounts, Gowadia led a relatively quiet existence. Following his retirement, he moved to Maui, Hawaii, where he and his wife built a luxury home on a cliff overlooking the ocean. However, Gowadia's activities were not as innocent as they appeared.

Though displaying the outward appearance of a retiree, Gowadia was actually working covertly

to help China design a cruise missile exhaust system that would allow the missile to evade detection. Between July 2003 and June 2005, Gowadia took six trips to China. He also established three foreign entities, including a fake children's charity in Liechtenstein, to disguise the income he received from foreign governments.

In August 2010, Gowadia was found guilty of 14 criminal violations, including illegally communicating classified national defense information, unlawfully exporting military technical information, illegally retaining defense information, money laundering, and filing false tax returns. He is currently serving a 32-year sentence for his crimes.

So, how did he do it? Were there any outward indicators of his secret double life? If any seemingly minor issues had been reported as adverse information along the way, the collection of suspicious behaviors may have come together sooner to reveal a more complete picture of this man who spent his retirement years betraying the U.S. government.

3. Suspicious Contacts

According to NISPOM subparagraph 1-302b, contractors must report all attempts to gain illegal or unauthorized access to classified information, all attempts to compromise a cleared employee, and all contacts between cleared employees and foreign intelligence officers. These are all known as suspicious contacts.

Why report suspicious contacts?

Suspicious contacts may suggest serious threats to national security. Taken individually, each unique incidence of suspicious contact may seem relatively innocuous. But collectively, reports of suspicious contacts can be combined from various sources to paint a much different picture, helping the government to identify patterns of suspicious activity that are much more pervasive than they may first appear.

In our modern world, which seems to be shrinking daily with technological advances that increase globalization, contact with foreign entities is a common occurrence. For the most part, this increased contact is a natural result of our new world economy. However, as a contractor entrusted to protect classified information, you must be vigilant in your monitoring of outside contacts.

Not all suspicious contacts are obvious; even seemingly benign interactions may be well-disguised attempts to infiltrate your facility and gain access to classified information. When you have reason to believe that a contact may be suspicious, you must report in writing to your IS Rep. If the situation is urgent, your initial report may be made by phone, but a written report must follow.

For more information on identifying suspicious contacts, refer to the *Thwarting the Enemy* Web-based training course offered by the DSS Academy.

a. Suspicious Indicators

There are several indicators of suspicious contacts that the FSO and all contractor employees should be aware of.

- The first is individuals or organizations making unsolicited requests for information about your company. Such requests may involve surveys or questionnaires being sent electronically to individuals within your facility.
- The second is individuals displaying inappropriate conduct during visits to your facility. This may include visitors having a hidden agenda or asking questions outside the scope of the visit.
- The third is suspicious offers to perform work for your company, such as foreign scientists, engineers, or interns offering their services for free.
- The fourth is foreign contact with individuals in your company based on their family origin.
- And the last is foreign organizations making contact with individuals within your facility.

Visit the DSS Counterintelligence Web site for further discussion on suspicious indicators.

Note that reporting suspicious contacts is the one exception to the general rule about reporting personnel issues to PSMO-I. Though often related to *people*, suspicious contacts are reported to your IS Rep because they are more likely to be targeting the *facility*.

4. Other Changes Affecting Personnel

In addition to the more serious reports about adverse information and suspicious contacts, you must also report administrative changes that may affect an employee's personnel security clearance. Each of these personnel-related reporting circumstances must be reported to PSMO-I via JPAS.

a. Changes in Cleared Employee Status

NISPOM subparagraph 1-302c lists certain changes in a cleared employee's status that must be reported. These reportable changes include the following:

- The death of a cleared employee
- A cleared employee changing his or her name
- The departure of a cleared employee from the company
- The change in citizenship status of a cleared employee

- A cleared employee no longer needing access to classified information

All changes in a cleared employee's status must be reported to PSMO-I using JPAS. These changes may be entered directly into JPAS.

b. Citizenship by Naturalization

If a non-U.S. citizen who has been granted limited access to classified information in the contractor facility becomes a U.S. citizen, then you must report details about that employee's naturalization. The following details must be reported: where the employee became a citizen, when the employee became a citizen, the name of the court that granted citizenship, and the employee's naturalization certificate number. Citizenship by naturalization must be reported to PSMO-I using the RRU function in JPAS.

c. Employees Desiring Not to Perform on Classified Work

Contractors must report cleared employees at contractor facilities who express a desire not to perform classified work. If an employee at your facility expresses a desire to not perform on classified work, then you must submit a report to PSMO-I. This includes employees who are being processed for a clearance and decide to discontinue the clearance process and employees who already hold clearances and would like to relinquish them. Employees who no longer wish to perform classified work must be reported to PSMO-I using the RRU function in JPAS.

d. Refusal to Execute Standard Form 312

Standard Form 312, or SF-312, the Classified Information Nondisclosure Agreement, is a required part of the personnel security clearance, or PCL, process. All cleared employees must sign this form prior to having access to classified information. Any cleared employee who refuses to complete and sign the SF-312 must be reported to PSMO-I using the RRU function in JPAS.

5. Job Aid

Take a moment to review this job aid, which summarizes the NISPOM requirements for reporting personnel changes.

NISPOM Paragraph	Reporting Topic	What to Report	How to Report	Report Recipient
1-302a	Adverse Information	Any information that raises doubt about the integrity or character of a cleared employee or that causes the DoD to question an individual's judgment, reliability, or suitability to have access to classified information; may include information about a cleared employee's— • Financial situation • Personal conduct • Allegiance to the United States • Reliance on drugs or alcohol • Criminal convictions NOTE: Refer to the DoD's Adjudicative Guidelines for Determining Eligibility for Access to Classified Information for a complete list. *Do not report information based on rumor or innuendo.*	Incident Report function in JPAS	PSMO-I
1-302b	Suspicious Contacts	• Efforts by any individual, regardless of nationality, to gain illegal or unauthorized access to classified information or to compromise a cleared employee • All contacts between cleared employees and foreign intelligence officers • All contacts that suggest that a cleared employee may be the target of an attempted exploitation by the intelligence officers of another country	In writing	IS Rep

NISPOM Paragraph	Reporting Topic	What to Report	How to Report	Report Recipient
1-302c	Change in Cleared Employee Status	The following changes in the personal status of a cleared employee: • Death • Change of name • Termination of employment • Change of citizenship • End of access to classified information	Enter changes directly into JPAS	PSMO-I
1-302d	Citizenship by Naturalization	All immigrant aliens with a Limited Access Authorization (LAA) who are granted U.S. citizenship through naturalization	Request to Research or Upgrade function in JPAS Report must include— • City, county, and state of naturalization • Date of naturalization • Court • Certificate number	PSMO-I
1-302e	Employees Desiring Not to Perform on Classified Work	• All employees who no longer wish to be processed for a clearance • All cleared employees who no longer wish to continue an existing clearance	Request to Research or Upgrade function in JPAS	PSMO-I
1-302f	Standard Form (SF) 312	Any cleared employee who refuses to execute the "Classified Information Nondisclosure Agreement" (SF-312)	Request to Research or Upgrade function in JPAS	PSMO-I

Changes Affecting the Facility

1. Reporting on the Facility

Let's look again at the 14 subparagraphs listed in NISPOM paragraph 1-302. In addition to the information and events affecting personnel security clearances, contractors must also report various types of information and events that could affect the facility's security clearance.

The NISPOM lists eight types of information or events that are related to the facility and may affect the facility's security clearance. Recall that reports about the facility are reported to your IS Rep at the DSS Field Office. Most are reported in writing directly to your IS Rep, but some may be reported electronically, using the electronic facility security clearance, or e-FCL, system. Let's look at each of these in closer detail.

2. Change Conditions Affecting the Facility Clearance

If a cleared contractor facility goes out of business, what becomes of the classified information the facility possessed or had access to? Where is it? Who has access to it? Are the cleared employees aware of their continuing responsibility to protect any information they may have had access to?

If a cleared contractor facility is purchased by a foreign owner, whose influence is the company under? Who has control over the company's classified programs?

These questions and more must be considered when certain changes occur at a cleared contractor facility. NISPOM paragraph 1-302g requires contractors to report the following change conditions that affect the facility's security clearance:

- Changes in company or facility ownership
- Changes in the name or address of the company or facility
- Changes to key management personnel, or KMPs
- Termination of company operations for any reason, including bankruptcy
- Actual or anticipated changes in foreign ownership, control, or influence, or FOCI.

When reporting changes in FOCI, you must submit a Certificate Pertaining to Foreign Interests, or Standard Form 328. Like other information affecting the facility, these change conditions are reported to your IS Rep. However, these are not reported directly to your IS Rep in writing. Instead, these changes are reported through the electronic facility security clearance, or e-FCL, system.

a. Key Management Personnel

Key management personnel, or KMPs, include more than just the presidents and FSOs of cleared contractor organizations. The specific job titles of the KMPs in your organization will vary, but may include the following:

- President or chief executive officer, commonly referred to as the CEO
- Vice presidents or division directors
- Facility security officer, or FSO
- Members and officers of the board of directors, including the chairman of the board, secretary, and treasurer
- Any stockholder in a position to exert control and influence over the organization's classified business operations.

When reporting changes in a facility's key management personnel, include the following information:

- Names and titles of the individuals being replaced
- The clearance status of the new KMPs, including—
    - Level of clearance
    - Date of clearance
    - Date and location of birth
    - Social security number
    - Citizenship
- Whether they have been excluded from access
- Whether they have been temporarily excluded from access while clearance is pending

It is important to note that even though changes in KMPs are reported to the IS Rep, any issues related to the personnel clearances of these KMPs should be reported to PSMO-I just like they are for any other cleared employee.

3. Other Changes Affecting the Facility

In addition to administrative changes about the facility, contractors must also report other circumstances affecting a facility's security clearance. Each of these facility-related reporting circumstances must be reported in writing to your IS Rep.

a. Changes in Storage Capacity

Any changes that might raise or lower the classification level of information your cleared facility is approved to protect must be reported in writing to your IS Rep. Such changes may include when a company that is currently approved to store classified material up to Secret receives a classified contract that requires safeguarding at the Top Secret level.

b. Inability to Safeguard Classified Material

Emergency situations that render a contractor facility incapable of protecting classified information must be reported immediately with a phone call to the IS Rep. The FSO should follow up with a written report when the situation is no longer an emergency.

c. Security Equipment Vulnerabilities

Any significant vulnerabilities in a facility's security equipment must be reported in writing to your IS Rep. This includes vulnerabilities in intrusion detection systems, or IDS, access control systems, communications security, or COMSEC, equipment or systems, and information system, or IS, security hardware and software.

d. Unauthorized Receipt of Classified Information

If a contractor facility receives or discovers any classified material that it is not authorized to have, then a written report must be submitted to your IS Rep. The report should include the following information: the source of the material, its origination, the quantity, the subject or title, the date, and the classification level.

e. Employee Information in Compromise Cases

When an employee is involved in the loss or compromise of classified information, the CSA may request information about the employee. When requested, this information must be reported in writing to your IS Rep. Specific reporting requirements regarding lost or compromised material will be covered in greater detail in the next lesson.

f. Disposition of Classified Materials Terminated From Accountability

If someone in your facility discovers classified material that was previously reported as lost, then you must submit a written report to your IS Rep.

g. Foreign Classified Contracts

Contractors sometimes negotiate and award contracts outside the purview of a government contracting activity, or GCA. If such precontract negotiations and contract awards involve the release of U.S. classified information to a foreign interest or access to classified information provided by a foreign interest, then they must be reported in writing to your IS Rep.

4. Job Aid

Take a moment to review this job aid, which summarizes the NISPOM requirements for reporting facility changes.

NISPOM Paragraph	Reporting Topic	What to Report	How to Report	Report Recipient
1-302g	Change Conditions Affecting the Facility Security Clearance	(1) Change of ownership	e-FCL	IS Rep (via e-FCL)
		(2) Change of name or address	e-FCL	
		(3) Change to information previously submitted for key management personnel (KMPs)	e-FCL • Submit a new KMP list	
		(4) Termination of business or operations	e-FCL	
		(5) Change in foreign ownership, control, or influence (FOCI)	e-FCL • Submit a revised "Certificate Pertaining to Foreign Interests" (SF-328) • Submit a copy of Schedule 13D, if received	
1-302h	Changes in Storage Capability	Any changes in the facility's storage capability that would raise or lower the level of classified information the facility is approved to safeguard	In writing	IS Rep
1-302i	Inability to Safeguard Classified Material	Any emergency situation that renders the facility incapable of safeguarding classified material	In writing	IS Rep
1-302j	Security Equipment Vulnerabilities	Significant vulnerabilities identified in security equipment, such as— • Intrusion detection systems (IDS) • Access control systems • Communications security (COMSEC) equipment or systems • Information system (IS) security hardware and software	In writing	IS Rep

NISPOM Paragraph	Reporting Topic	What to Report	How to Report	Report Recipient
1-302k	Unauthorized Receipt of Classified Material	The receipt or discovery of any classified material that the contractor is not authorized to have	In writing Report should identify— • Source (sender) • Originator (generated material) • Quantity (pages, volumes) • Subject or title • Date material was generated • Classification level (markings)	IS Rep
1-302l	Employee Information in Compromise Case	Information concerning an employee in connection with the loss, compromise, or suspected compromise of classified information NOTE: Report upon request of CSA only.	In writing	IS Rep
1-302m	Disposition of Classified Material Terminated From Accountability	The discovery of classified material that was previously reported as lost	In writing	IS Rep
1-302n	Foreign Classified Contracts	Any precontract negotiation or award not placed through a GCA that involves or may involve— (1) The release or disclosure of U.S. classified information to a foreign interest (2) Access to classified information furnished by a foreign interest	In writing	IS Rep

Review Activity 1

NISPOM paragraph 1-302 has 14 subparagraphs listing different types of events and information that must be reported to the CSA. Of the six listed below, decide for each whether it should be reported to PSMO-I or to your IS Rep at the DSS Field Office assigned to your facility. Check your answers in the Answer Key at the end of this Student Guide.

	PSMO-I	IS Rep
Adverse information	○	○
Suspicious contacts	○	○
Change in cleared employee status	○	○
Citizenship by naturalization	○	○
Unauthorized receipt of classified material	○	○
Employee information in compromise cases	○	○

Review Activity 2

According to NISPOM paragraph 1-302g, which of the following should be reported as a change condition that might affect a contractor's facility security clearance? Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ The company has hired 11 new employees to meet growing business needs.
- ○ The facility's alarm system has been malfunctioning.
- ○ The company has merged with another company and is under new ownership.
- ○ The company has just won a major contract.

Review Activity 3

Which of the following events should be reported to PSMO-I? Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- ☐ Dana received a package containing classified material that was intended for another person.
- ☐ Helen Bernard got married and changed her name to Helen Healy.
- ☐ Martin Lundberg, who currently holds an LAA, became a U.S. citizen through naturalization.
- ☐ Nathan purchased a new home and moved from Virginia to Maryland.
- ☐ Walt was arrested and charged with driving under the influence.
- ☐ Janet received a request for classified information from an uncleared person she met at a conference.

Answer Key

Review Activity 1

NISPOM paragraph 1-302 has 14 subparagraphs listing different types of events and information that must be reported to the CSA. Of the six listed below, decide for each whether it should be reported to PSMO-I or to your IS Rep at the DSS Field Office assigned to your facility.

	PSMO-I	IS Rep
Adverse information	●	○
Suspicious contacts	○	●
Change in cleared employee status	●	○
Citizenship by naturalization	●	○
Unauthorized receipt of classified material	○	●
Employee information in compromise cases	○	●

Review Activity 2

According to NISPOM paragraph 1-302g, which of the following should be reported as a change condition that might affect a contractor's facility security clearance?

- ○ The company has hired 11 new employees to meet growing business needs.
- ○ The facility's alarm system has been malfunctioning.
- ⊙ The company has merged with another company and is under new ownership.
- ○ The company has just won a major contract.

Rationale: According to NISPOM paragraph 1-302g, you must report a change in company ownership. You must also report changes in the name or address of the company or facility, changes to key management personnel (KMPs), termination of company operations for any reason, and changes in foreign ownership, control, or influence (FOCI).

Review Activity 3

Which of the following events should be reported to PSMO-I?

- ☐ Dana received a package containing classified material that was intended for another person
- ☒ Helen Bernard got married and changed her name to Helen Healy.
- ☒ Martin Lundberg, who currently holds an LAA, became a U.S. citizen through naturalization.
- ☐ Nathan purchased a new home and moved from Virginia to Maryland.
- ☒ Walt was arrested and charged with driving under the influence.
- ☐ Janet received a request for classified information from an uncleared person she met at a conference.

Rationale:

Event 1: Dana was an unauthorized recipient of classified material, which must be reported to the IS Rep. (NISPOM 1-302k)

Event 2: Helen's name change should be reported to PSMO-I. (NISPOM 1-302c)

Event 3: Martin became a citizen by naturalization, which must be reported to PSMO-I. (1-302d)

Event 4: Nathan's change in personal residence does not need to be reported.

Event 5: Walt's abuse of alcohol shows questionable judgment and is considered adverse information, which should be reported to PSMO-I. (NISPOM 1-302a)

Event 6: Janet has received a suspicious contact, which must be reported to the IS Rep. (NISPOM 1-302b)

Student Guide

Course: NISP Reporting Requirements

Lesson 4: Reporting Security Concerns and Violations

Lesson Introduction

1. Objectives

In addition to reporting changes related to personnel and facility security clearances, the facility security officer, or FSO, must also report security violations and other events involving actual or suspected espionage, sabotage, terrorism, and subversive activities. In this lesson, you will learn what qualifies as a security threat or violation. You will also learn how and where such threats and violations are to be reported. Here are the lesson objectives:

- Identify the circumstances requiring reporting that—
    - Affect the proper safeguarding of classified information
    - Indicate that classified information may have been lost or compromised
- Identify the reports that are required by the NISPOM
- Identify the reporting process for each type of information

2. Overview of Security Threats and Violations

Security threats and violations carry with them the potential for serious harm to our national security. But what exactly are these threats and violations? How are they defined? And what exactly must the contractor report?

National security threat: *An entity capable of aggression or harm to the U.S.*

A threat to our national security is any individual or group that is capable of aggression or harm to our country. Vigilant reporting of personnel and facility changes, especially with regard to adverse information and suspicious contacts, is one way to ward off potential threats to our national security. But the FSO must also report any information concerning known or suspected espionage, sabotage, terrorism, or subversive activities as well as any security violations that may occur at their facility.

Security violation: *An action that could result in unauthorized disclosure of classified information*

A security violation is any knowing, willing, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. Remember that the overall purpose of the NISP is to ensure the protection of classified information released to industry. Therefore, any failure on the part of industry to protect that classified information is considered a violation. The FSO must report any violations that result in the loss, compromise, or suspected compromise of classified information.

Individual culpability: *Individual responsibility for a security violation*

A cleared employee is always responsible for incidents resulting in security violations. If the responsible individual can be identified and has shown a deliberate disregard for security requirements, gross negligence in the handling of classified material, or a pattern of negligence or carelessness, then the FSO must also file an individual culpability report. Let's look at each of these reporting categories in closer detail.

Reporting National Security Threats

1. Espionage, Sabotage, Terrorism, and Subversive Activities

Although many types of threats exist, the NISPOM specifically addresses four that contractors must report. NISPOM paragraph 1-301 requires contractors to report to the FBI any known information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities.

As the FSO, if you have any reason to suspect any of these activities, then you must report it to the nearest FBI field office. If the matter is urgent or suggests an imminent danger, then the initial report may be made by phone, but a written report must follow. Note that when reporting to the FBI, the FSO should not act without direction from the FBI!

The FBI will investigate all reports and will determine what, if any, further action is appropriate. It may also refer the situation to another government agency. When submitting your final report to the FBI, you must also provide a copy of the written report to the DSS Field Office assigned to your facility. This informational copy should be submitted to your Industrial Security Representative, or IS Rep.

a. Espionage

Espionage: *The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent to injure the U.S.*

Commonly known as spying, espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense

with an intent, or with reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation.

The most famous espionage cases are those involving government insiders, such as the case of Aldrich Ames, a 31-year veteran of the CIA who spied for Russia for nine years.

However, there have been several well-known espionage cases involving contractor personnel as well. Consider the case of Chi Mak: An electrical engineer for a U.S. defense contractor, Mak worked on more than 200 U.S. defense and military contracts over a 20-year span. In 2008, Mak was convicted of acting as an unregistered foreign agent to China and conspiring to export technology related to U.S. Navy ships.

b. Sabotage

Sabotage: *The deliberate destruction, disruption, or damage of equipment, resources, or services*

In general terms, sabotage is the deliberate destruction, disruption, or damage of equipment, resources, or services. Sabotage can take different forms in different contexts.

In the context of national security, sabotage refers specifically to any act with the intent to injure, interfere with, or obstruct the national defense of a country by willfully damaging or destroying, or attempting to damage or destroy, any national defense or war materials, premises, or utilities, including human and natural resources.

c. Terrorism

Terrorism: *The calculated use of unlawful violence or the threat of unlawful violence to instill fear*

The threat that often hits closest to home, terrorism is the calculated use of unlawful violence or the threat of unlawful violence to instill fear. It is intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

As we have seen in several high-profile cases in recent years, acts of terrorism can strike anywhere. They can be committed by individuals or by organizations. And they can be attributed to any number of causes.

The 1988 bombing of Pan Am flight 103 over Lockerbie, Scotland, was a foreign attack in a foreign country, but theories suggest that the actual target was the

U.S. government. The 1995 Oklahoma City bombing of the Alfred P. Murrah Federal Building was a domestic attack by a U.S. citizen who was motivated by his hatred of the federal government. And the September 11th attacks on the World Trade Center and the Pentagon were foreign attacks by an extremist organization making a statement against our society, our economy, and our way of life.

d. Subversive Activities

Subversive Activities: *Willful acts that are intended to be detrimental to the best interests of the government*

Subversive activities are willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage. Any activities that support lending aid, comfort, and moral support to individuals, groups, or organizations that advocate the overthrow of the government by force and violence are considered subversive activities.

Examples of subversive activities include holding an active membership in hate groups or extremist organizations such as the Ku Klux Klan or Aryan Nations, paying dues to maintain membership in such organizations even if not actively participating in the organization, and participating in protests or rallies in support of such organizations even if not an actual dues-paying member.

Reporting Security Violations

1. Security Violations

The NISPOM defines a security violation as the failure to comply with the policy and procedures established by the NISPOM that reasonably could result in the loss or compromise of classified information. In other words, a security violation is any knowing, willing, or negligent action that could result in the unauthorized disclosure of classified information.

Examples of security violations include—

- Leaving a classified storage container open and unattended
- Allowing unauthorized individuals access to classified material
- Allowing unauthorized individuals access to combinations for containers authorized to store classified material
- Sending classified material by unsecured fax
- Removing classified material from the facility without permission from the FSO

- Copying or destroying classified material without proper authorization
- Using an unaccredited computer to process classified information

Be aware that this final example accounts for most violations that occur today. Each of these examples renders classified information vulnerable to loss, compromise, or suspected compromise.

Even if the classified material in question is not actually lost or compromised, each of these events allows the opportunity for possible compromise and must be investigated. The requirement for reporting security violations is defined in NISPOM paragraph 1-303, which describes the general process for reporting the loss, compromise, or suspected compromise of classified information. Any violations that result in the loss, compromise, or suspected compromise of classified information must be reported to your IS Rep.

a. Loss

Classified information is considered lost when it is out of a cleared employee's control and cannot be located or when its location cannot be determined.

A loss involves classified information that is—

- Outside the custodian's control and cannot be located
- Of a disposition that cannot be determined

Note: Classified information sent by unencrypted e-mail or sent over an unapproved LAN or WAN is considered to be lost

b. Compromise

Classified information is considered compromised when disclosure to an unauthorized individual can be confirmed.

A compromise is a confirmed disclosure of specifically identifiable classified information to specified unauthorized individual(s)

c. Suspected Compromise

Suspected compromise occurs when an unauthorized individual may have had the opportunity to access classified information but when actual disclosure cannot be confirmed.

A suspected compromise occurs whenever identifiable classified information has been made available to unauthorized individual(s) who may have gained access to the information. Proving that there was unauthorized access to the information

may be difficult, but the facts lead a reasonable person to reasonably conclude that unauthorized access probably occurred.

Example: Storage of classified information in unsecured areas for extended periods during which unauthorized personnel had unrestricted or unmonitored access.

2. Reporting Process

When reporting actual security violations resulting in the loss, compromise, or suspected compromise of classified information, you will report directly to your IS Rep at the DSS Field Office. Suggested timeframes for reporting are provided here, but ultimately, the reporting deadlines will be determined by your IS Rep.

When the FSO has reason to believe that classified information has been lost or compromised, the first step in reporting is to initiate a preliminary inquiry. If the preliminary inquiry concludes that there was no compromise, then the FSO must complete the inquiry and file it away for review by the IS Rep in the facility's next government security inspection. If the preliminary inquiry confirms that a loss, compromise, or suspected compromise has occurred, then the FSO must prepare an initial written report, which is generally submitted by the close of business on the following work day.

In preparing the final report, the FSO should use the General Administrative Inquiry Guidance to perform a thorough investigation of the security violation. The final report is generally submitted within 15 calendar days following submission of the initial report.

a. Preliminary Inquiry

The first step in reporting security threats and violations is to conduct a preliminary inquiry. The purpose of the preliminary inquiry is to secure the classified information, ascertain as much information as possible, and determine whether a loss, compromise, or suspected compromise actually occurred.

In conducting the preliminary inquiry, the FSO should assume the role of investigator, assessing the who, what, when, where, why, and how, analyzing possible causes, and determining who is responsible. The FSO should also decide on a corrective action.

The preliminary inquiry should begin as soon as the FSO has reason to believe that a violation has occurred.

Elements of preliminary inquiry

- Ascertain facts
  - Who, what, when, where, why, and how
- Analyze the cause
- Determine culpable party
- Determine corrective action

a. Initial Report

The second step in reporting security threats and violations is to prepare an initial report.

Loosely following the General Administrative Inquiry Guidance, the initial report should contain as much information as is available at the time. This is not a comprehensive report and does not require a thorough investigation. It is intended simply to give the government a broad overview of the investigation that is underway.

The initial report is generally submitted to your IS Rep within one business day of the preliminary inquiry.

Contents of initial report

- All facts as known

b. Final Report

The third and final step in the reporting process is to prepare the final report.

Closely following the General Administrative Inquiry Guidance, the final report should contain a comprehensive description and analysis of all circumstances that necessitated the investigation.

The final report must be submitted in writing to your IS Rep upon completion of your detailed inquiry. It is generally submitted within 15 calendar days of the initial report, but the actual deadline will be determined by your IS Rep.

Contents of final report

- Reference to initial report
- Description of material that was lost of compromised
  - Originating activity
  - Date of origin
  - Document title
  - Number of pages
  - Description of contents
  - Associated contract or program
  - Classification level
- Essential facts of the incident
  - Who, what, when, where, why, and how
- Personal information about responsible party
  - Name
  - Position
  - SSN
  - Place and date of birth
  - Date PCL or LAA granted
  - Record of any prior incidents for which individual was deemed responsible
- Description of how information was first reported
  - Name of person who reported
  - Name of person receiving report
  - Date of first report
- Statement of action taken
  - What action was taken to secure material and limit any further damage after discovery?
- List of all lost or unaccounted classified information*
- Description of circumstances surrounding vulnerability of classified information
  - When and how long was classified information vulnerable to unauthorized disclosure?
  - How did information become vulnerable to unauthorized disclosure?
  - Who had access during period of vulnerability?
- Conclusion with supporting rationale
  - Loss
  - Compromise
  - Suspected compromise
  - No compromise

Contents of final report (continued)

- Statement of corrective action
  - What actions have been taken to prevent similar incidents?
- Statement of disciplinary action
  - What disciplinary action, if any, was taken against the responsible individual?

**Note that this information could render the final report classified.*

Reporting Individual Culpability

1. Individual Culpability

The final reporting requirement described in the NISPOM covers individual culpability reports. According to NISPOM paragraph 1-304, an individual culpability report is required when individual responsibility for a security violation can be determined and one of the following conditions exists: if the violation involved a deliberate disregard for security requirements, if the violation involved gross negligence in the handling of classified material, or if the violation involved was not necessarily deliberate in nature but is part of an ongoing pattern of negligence or carelessness.

Individual culpability reports do not replace reports on security violations. In fact, if an individual is determined to be responsible for a security violation, then an individual culpability report must be submitted in addition to the security violation report. Like the other personnel-related reports discussed in Lesson 3, individual culpability reports are submitted to PSMO-I using the incident report function in JPAS.

It is important to note that every cleared contractor facility must have in place a graduated scale of administrative actions to be taken against employees who are found to be responsible for security violations. When reporting individual culpability, a statement about any administrative actions taken against the responsible employee must be included in your report to PSMO-I.

Contractors must report activities that show—

- Deliberate disregard
- Gross negligence
- Pattern of negligence or carelessness

Reporting Security Concerns and Violations

1. Job Aid

Take a moment to review this job aid, which summarizes the NISPOM requirements for reporting security threats, security violations, and individual culpability.

NISPOM Paragraph	Reporting Topic	What to Report	How to Report	Report Recipient
1-301	Espionage Sabotage Terrorism Subversive Activities	Any known information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any of the contractor's sites	In writing NOTE: If the matter is urgent, make initial report by phone, and follow up with a written report to the FBI. Send an informational copy to your IS Rep at the DSS Field Office.	FBI Send informational copy to IS Rep
1-303	Loss, Compromise, or Suspected Compromise	Any security violations resulting in the loss, compromise, or suspected compromise of classified information NOTE: If the preliminary inquiry finds no compromise, then the completed inquiry should be filed away for review by your IS Rep in the next facility security inspection.	• Initial Report (in writing) • Final Report (in writing)	IS Rep
1-304	Individual Culpability Report	Determination of individual responsibility for a security violation combined with evidence of one or more of the following factors: a. Deliberate disregard of security requirements b. Gross negligence in the handling of classified material c. A pattern of negligence or carelessness	Incident Report function in JPAS Report should include— • Statement of the administrative actions against the employee • Details of the incident(s)	PSMO-I

Review Activity 1

Which of the following should be reported to the FBI? Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- ☐ A cleared employee just married a citizen of a foreign country.
- ☐ You have inconclusive evidence that an employee may have sold classified materials to alleviate his financial stress.
- ☐ A safe containing classified information appears to have been tampered with.
- ☐ A cleared employee is planning an extended vacation to Israel.
- ☐ There was a small explosion in your classified facility's server room. No materials were compromised. It is not clear what caused the explosion, but circumstances cause you to believe that it may not have been an accident.

Review Activity 2

NISPOM subparagraph 1-304 lists the requirements for reporting individual culpability. Which of the following cleared employees do you think should be reported? Select Report or Do Not Report for each statement. Check your answers in the Answer Key at the end of this Student Guide.

	Report	**Do Not Report**
Dan took classified information home with him over the weekend. He knew it was a security violation, but he was trying to meet a deadline. This was his first violation.	○	○
Marie is usually vigilant in her work, but after working late one night, she finished working with a Secret document after the security container had been closed. Not knowing the combination, she locked the document in her desk drawer instead of finding someone who could put it in the appropriate container.	○	○
Alex accidentally left a file out on his desk when he went to lunch. The only person in the area during that time was another cleared employee. This was his first violation.	○	○
Jill did not properly secure her storage container four times over the past six months even though she has been instructed repeatedly on proper storage procedures.	○	○

Review Activity 3

A security violation is any knowing, willing, or negligent action that could result in the loss, compromise, or suspected compromise of classified information. Which of the following are reportable as an example of loss, compromise, or suspected compromise? Select Reportable or Not Reportable for each statement. Check your answers in the Answer Key at the end of this Student Guide.

	Reportable	**Not Reportable**
Rafael was overheard discussing classified information with a colleague during his morning coffee break in the building cafeteria.	○	○
Nancy left classified information out on a desk in an unsecured room where uncleared individuals could see the information.	○	○
Donna left a safe containing classified material open and unattended, though there is no confirmation that any classified information was disclosed.	○	○
Shane left a GSA security container unsecured in an approved closed area.	○	○
Richard sent classified information by e-mail from an unaccredited computer.	○	○

Answer Key

Review Activity 1

Which of the following should be reported to the FBI?

- ☐ A cleared employee just married a citizen of a foreign country.
- ☒ You have inconclusive evidence that an employee may have sold classified materials to alleviate his financial stress.
- ☒ A safe containing classified information appears to have been tampered with.
- ☐ A cleared employee is planning an extended vacation to Israel.
- ☒ There was a small explosion in your classified facility's server room. No materials were compromised. It is not clear what caused the explosion, but circumstances cause you to believe that it may not have been an accident.

Review Activity 2

NISPOM subparagraph 1-304 lists the requirements for reporting individual culpability. Which of the following cleared employees do you think should be reported?

	Report	**Do Not Report**
Dan took classified information home with him over the weekend. He knew it was a security violation, but he was trying to meet a deadline. This was his first violation.	●	○
Marie is usually vigilant in her work, but after working late one night, she finished working with a Secret document after the security container had been closed. Not knowing the combination, she locked the document in her desk drawer instead of finding someone who could put it in the appropriate container.	●	○
Alex accidentally left a file out on his desk when he went to lunch. The only person in the area during that time was another cleared employee. This was his first violation.	○	●
Jill did not properly secure her storage container four times over the past six months even though she has been instructed repeatedly on proper storage procedures.	●	○

Rationale:

Event 1: Even though it is his first violation, Dan should be reported because he deliberately disregarded the rules.

Event 2: Even though she is usually vigilant in her work, Marie should be reported because she has committed an act of gross negligence.

Event 3: Alex should not be reported because this was his first violation and there was no evidence of gross negligence or deliberate disregard for the rules.

Event 4: Jill should be reported because she has shown a pattern of carelessness.

Review Activity 3

A security violation is any knowing, willing, or negligent action that could result in the loss, compromise, or suspected compromise of classified information. Which of the following are reportable as an example of loss, compromise, or suspected compromise?

	Reportable	**Not Reportable**
Rafael was overheard discussing classified information with a colleague during his morning coffee break in the building cafeteria.	●	○
Nancy left classified information out on a desk in an unsecured room where uncleared individuals could see the information.	●	○
Donna left a safe containing classified material open and unattended, though there is no confirmation that any classified information was disclosed.	●	○
Shane left a GSA security container unsecured in an approved closed area.	○	●
Richard sent classified information by e-mail from an unaccredited computer.	●	○

Rationale:

Event 1: Talking in public about classified information is reportable as compromise, because disclosure of classified information can be confirmed.

Event 2: Leaving classified information out in the open in an unsecured location where uncleared individuals can see the information is reportable as compromise, because disclosure of classified information can be confirmed.

Event 3: Leaving a safe containing classified material open and unattended is reportable as suspected compromise, because the material was open to disclosure but disclosure cannot be confirmed.

Event 4: Leaving a GSA-approved security container unsecured in an approved closed area is not reportable because its contents were never open to disclosure.

Event 5: Sending classified information by unencrypted e-mail or over an unapproved LAN or WAN is always considered a loss and should be reported

Student Guide

Course: NISP Reporting Requirements

Lesson 5: Course Conclusion

Course Summary

As you have learned, reporting is a critical responsibility of the facility security officer, or FSO, in helping to protect classified information and ultimately in safeguarding national security. During this course you learned about the reporting structure of the National Industrial Security Program, or NISP, as well as the types of information required to be reported and the reporting mechanisms for each type of information.

You learned about—

- The role of the facility security officer (FSO)
- The reporting structure of the NISP
- Why to report, what to report, and how to report

Lesson Review

Here is a list of the lessons in the course:

- Understanding Reporting in the NISP
- Reporting Personnel and Facility Changes
- Reporting Security Concerns and Violations

Course Objectives

You should now be able to—

- ✓ Identify the importance of reporting and the potential effects that failure to report can have on national security and the warfighter
- ✓ Identify the legal and regulatory basis for NISP reporting requirements
- ✓ Identify the circumstances requiring reporting that—
    - o Affect the status of the facility security clearance (FCL), including attempts by suspicious contacts to gain access to classified information
    - o Affect the status of the personnel security clearance (PCL), including attempts by suspicious contacts to compromise a cleared employee

- Affect the proper safeguarding of classified information
- Indicate that classified information may have been lost or compromised

✓ Identify the reports that are required by the NISPOM

✓ Identify the reporting process for each type of information

Course Conclusion

Congratulations. You have completed the *NISP Reporting Requirements* course.

To receive credit for this course, you must take the *NISP Reporting Requirements* examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.