NISP Reporting Requirements v2

Student Guide

September 2017

Center for Development of Security Excellence

Lesson 1: Course Introduction

Course Introduction

Course Information

The purpose of the course is to 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.

The audience includes:

- Facility security officers (FSOs) at cleared DoD contractor facilities participant in the NISP
- Other contractor security personnel
- DSS Industrial Security Representatives (IS Reps)
- DoD Industrial Security Specialists

The course requires a 75% on the final examination to pass.

Estimated completion time is 75 minutes.

Course Overview

The National Industrial Security Program (NISP) is a government-industry partnership that was forged to ensure the protection of classified information in the possession of industry. One method used to ensure this protection is through the required NISP Operating Manual (NISPOM) reporting requirements. These reporting requirements pose many challenges to the Facility Security Officer (FSO). Some of the challenges include changing the culture at their company from one of non-reporting to one of reporting, ensuring employees are aware of the required reports they need to make, and then making sure employees understand exactly what they need to report and how to report it.

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:

- Describe reporting requirements for National Industrial Security Program (NISP) contractors

- Identify procedures for reporting certain events that affect personnel or facility clearances
- Recognize procedures for reporting security violations and national security threats

Course Structure

This course is organized into the lessons listed here:

- Course Introduction
- Understanding Reporting in the NISP
- Reporting Personnel and Facility Changes
- Security Violations and Reports to the FBI
- Course Conclusion

Lesson 2: Understanding Reporting in the NISP

Lesson Introduction

Importance of Reporting

You've heard the stories of Edward Snowden, former Central Intelligence Agency employee and former contractor for the U.S. government who copied and leaked classified information from the National Security Agency without authorization. But what about Walter Liew, Hannah Robert and Wen Chyu Liu? Each of these individuals provided information to foreign countries for financial gain.

In light of this information, 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?

Walter Liew conspired with at least two current and former DuPont employees to steal the company's chemical trade secrets to sell to China. Hannah Roberts stole export controlled drawings of parts used in the torpedo systems for nuclear submarines, military attack helicopters, and F-15 fighter aircraft to sell to India via her church website. Wen Chyu Liu worked for Dow Chemical and conspired with at least four current and former employees to steal elastomer trade secrets and sell to China.

Each of these individuals made significant financial gains through their crimes and traveled extensively overseas. Did any employees who worked with these individuals notice these incidents? If these incidents had been reported earlier, then it might have been possible to prevent a significant loss of classified information.

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

Objectives

Before you learn the specifics of how and what a Facility Security Officer (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:

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

Reporting Requirements

Why You Must Report

Is reporting really necessary? After all, 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 (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 Department of Defense (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 (NISPOM).

The NISPOM establishes the baseline security 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 certain events to the appropriate government agencies. This requirement includes both your own observations and those of your cleared employees. This requirement to report applies to certain events that:

- Impact the status of the contractor's Facility Security Clearance (FCL)
- Impact the status of an employee's Personnel Security Clearance (PCL)
- May indicate an employee poses an insider threat
- Affect the appropriate safeguarding of classified information
- Indicate that classified information has been lost or compromised

As a cleared contractor in the NISP, your company agrees to comply with all applicable NISPOM requirements, including the requirements to report. As your company's FSO, the responsibility to report these events belongs to you.

But that is only half of your reporting responsibility! You also have the responsibility to ensure your cleared employees are aware of their individual reporting responsibilities to include what needs to be reported and how to make these reports. After all, you can only submit reports on information you are aware of, and, for many of these reports you will be relying on your cleared employees to bring these matters to your attention.

What You Must Report

The NISPOM lists the various events that must be reported. The easiest way to understand these reports is to group them by where each report will be submitted, which also happens to be the way they are described in NISPOM paragraphs 1-301 through 1-304. According to the NISPOM, reports are submitted to either the Federal Bureau of Investigation (FBI) or the

Cognizant Security Agency (CSA). For the DoD and Department of Homeland Security (DHS), the CSA reports are submitted to the Defense Security Service (DSS) with certain reports going to your DSS Industrial Security Representative (IS Rep) and certain reports to the Personnel Security Management Office for Industry (PSMO-I). We will discuss this in greater detail later in this course but for now all you need to know is that all NISPOM required reports are submitted to either the FBI or the CSA.

Reporting Methods

Structure in the NISP

To best understand how to meet the NISPOM reporting requirements, 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 CSA has been authorized to establish an Industrial Security Program for the protection of classified information that has been entrusted to industry. Although, the CSA is responsible for NISP oversight, it may delegate a Cognizant Security Office (CSO) to administer the NISP on its behalf. DSS is delegated as the CSO for the DoD and DHS.

On the industry side, each cleared contractor facility must appoint an FSO, who is responsible for the overall administration of the security program and for ensuring appropriate reports are made in a timely manner. The FSO is the link between government and industry. The FSO is responsible for reporting events they have directly witnessed, and ensuring their cleared employees are making the appropriate required reports. Not only is the FSO responsible for ensuring that their cleared employees are aware of the NISPOM reporting requirements, they must also ensure their employees know what information should be reported and how to make reports. Once a report is received by the FSO, it is then up to the FSO to submit the reports to either the CSA or the FBI.

For the purposes of this course, we will focus on the reporting structure and processes as they apply specifically to the DoD and DHS, or CSA.

The majority of NISPOM reports will be submitted to the Defense Security Service (DSS), acting as the CSO on behalf of your CSA. Depending on the type of information that is being reported, CSA reports are generally submitted to one of two DSS entities. The first one being the DSS IS Rep assigned to your facility who will receive reports that may impact your FCL and safeguarding capability while PSMO-I will receive reports that may impact the PCLs of your cleared employees.

Refer to Appendix B for a job aid on the NISP reporting structure.

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 supplied in a designated format.

Remember, for the DoD and DHS, NISPOM reports designated to be sent to the CSA are submitted to DSS. The type of information being reported will determine which DSS entity will receive the report. Reports affecting PCLs are submitted to the PSMO-I while reports affecting your FCLs and/or safeguarding capabilities are submitted to the DSS IS Rep. Depending on the nature of the report, the DSS IS Rep may further disseminate the report to other DSS entities such as the Counterintelligence Special Agent (CISA) and the Information System Security Professional/Security Control Assessor (ISSP/SCA).

And finally, reports involving actual or suspected espionage, sabotage, terrorism, or subversive activities must be submitted to the FBI, with a copy sent to your DSS IS Rep. In matters of national security significance, reports may also be made to a hotline, as listed in the NISPOM paragraph 1-208. It is your responsibility to know the details so that you can gather the appropriate information from your own observations as well as from your cleared employees.

PSMO-I

Reports affecting personnel and reports affecting personnel security clearances are submitted to PSMO-I using the DoD System of Record.

DoD System of Record: Formerly the Joint Personnel Adjudication System (JPAS), but replaced by the Defense Information System for Security (DISS)

DSS IS Rep

Reports affecting the FCL and your ability to protect classified information are sent to the DSS IS Rep. These reports are submitted either in writing, by letter or e-mail, directly to the DSS IS Rep or through the electronic Facility Security Clearance (e-FCL) system.

FBI

Although you will submit the majority of your reports to DSS as the CSA, 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 you provide the DSS IS Rep a copy of the report submitted to the FBI. See Lesson 4 for additional details.

CSA Hotlines

CSA Hotlines (NISPOM 1-208)

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

DOE Hotline:
Department of Energy
Office of Inspector General
1000 Independence Avenue, SW
Room SD-031
Washington, DC 20585
(202) 586-4073
(800) 541-1625

DNI Hotline:
Director of National Intelligence
Office of Inspector General
Washington, DC 20505
(703) 482-2650

Review Activity

Review Activity 1

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

Select all that apply. Check your answer 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 service members.

Review Activity 2

Several regulatory and legal documents form the basis for the requirements to report.

Select the appropriate document for each statement. Check your answer in the Answer Key at the end of this Student Guide.

Question 1 of 3: The baseline security requirements (including the requirement to report) that ensure protection of classified information by contractors

- ○ E.O. 12829
- ○ DD Form 441
- ○ NISPOM

Question 2 of 3: Established the partnership between the U.S. government and private industry that is known as the National Industrial Security Program

- ○ E.O. 12829
- ○ DD Form 441
- ○ NISPOM

Question 3 of 3: The contractual agreement in which contractors agree to maintain minimum security controls to protect classified information

- ○ E.O. 12829
- ○ DD Form 441
- ○ NISPOM

Review Activity 3

Different types of information require reporting to different government entities.

Select the appropriate type of information for each entity to which it must be reported. Check your answer in the Answer Key at the end of this Student Guide.

Question 1 of 3: PSMO-I

- ○ Actual or suspected espionage, sabotage, terrorism, or subversive activities
- ○ Changes to personnel information
- ○ Changes to facility information

Question 2 of 3: DSS IS Rep

- ○ Actual or suspected espionage, sabotage, terrorism, or subversive activities
- ○ Changes to personnel information
- ○ Changes to facility information

Question 3 of 3: FBI

- ○ Actual or suspected espionage, sabotage, terrorism, or subversive activities
- ○ Changes to personnel information
- ○ Changes to facility information

Lesson 3: Reporting Personnel and Facility Changes

Lesson Introduction

Objectives

As the Facility Security Officer (FSO), you are required to report on various conditions related to both personnel and facility clearances. In this lesson, you will learn what events require reporting and how each is to be reported.

Here are the lesson objectives:

- Identify events requiring reporting that impact the status of the Facility Clearance (FCL)
- Examine events requiring reporting that impact the status of an employee's Personnel Security Clearance (PCL)
- Describe the reporting process for various required reports

Overview of Personnel and Facility Changes

NISPOM paragraph 1-302 identifies the various types of personnel-and facility-related information and events that must be reported to the Cognizant Security Agency (CSA).

NISPOM 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 Employee 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

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. In general, reports about personnel are made to the CSA. In general, reports about personnel are made to the PSMO-I, using the appropriate function in the DoD System of Record. Reports about the facility, including any changes in the company's Key Management Personnel (KMPs), are made to the DSS IS Rep assigned to the facility. These reports are submitted either in writing directly to the DSS IS Rep or through the electronic Facility Security Clearance (or e-FCL) system.

DoD System of Record: Formerly the Joint Personnel Adjudication System (JPAS), but replaced by the Defense Information System for Security (DISS)

Changes Affecting Personnel

Reporting on People

Of the various subparagraphs listed in NISPOM paragraph 1-302, there are several types of information or events related to personnel that may impact an individual employee's personnel clearance. Most reports about cleared personnel are reported to PSMO-I via the appropriate function in the DoD system of record. The one exception is reports about suspicious contacts, which are reported to the DSS IS Rep. Let's look at each of these in closer detail.

DoD System of Record: Currently the Joint Personnel Adjudication System (JPAS), but will soon be replaced by the Defense Information System for Security (DISS)

Adverse Information

Of all the reports that an FSO is responsible for, adverse information reporting is one of the most important. Adverse information refers to any behavior that might cause the DoD to question whether an individual should continue to have access to classified information. Adverse information can also be an indicator of an insider threat which is why it is important that you not only have a system in place to report adverse information using the appropriate function in the DoD System of Record, but that your employees understand what is meant by the term adverse information and how to report it. Specific reporting requirements can be found on the course resource page.

What types of information might be considered as adverse? 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.

NISPOM subparagraph 1-302a defines the NISP requirement to report adverse information. If you receive or become aware of any credible adverse information about yourself or any cleared employee, then you must report it to the Personnel Security Management Office for Industry (PSMO-I) using the appropriate function for incident reporting in the DoD System of Record. ***Do not*** report information based on rumor or innuendo. It is also your responsibility to ensure your cleared employees not only know their reporting responsibilities, but understand what needs to be reported and how to report.

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 (PCL).

DoD System of Record: Currently the Joint Personnel Adjudication System (JPAS), but will soon be replaced by the Defense Information System for Security (DISS)

National Security Adjudicative Guidelines

The FSO should be familiar with the National Security Adjudicative Guideline contained in the Security Executive Agent Directive 4, because the factors that determine an employee's qualification to be ***granted*** a clearance eligibility are the same factors that determine an employee's qualification to ***maintain*** a clearance eligibility. These factors include discussion of the following categories:

- Allegiance to the United States
- Foreign influence
- Foreign preference
- Sexual behavior
- Personal conduct
- Financial considerations
- Alcohol consumption
- Drug involvement and substance misuse
- Psychological conditions
- Criminal conduct
- Handling protected information
- Outside activities
- Use of information technology

Case Study

The case of James Michael Wells illustrates the importance of reporting adverse information.

Wells was a civilian employee at Coast Guard Communications Station in Kodiak, Alaska who exhibited several risk indicators including:

- Frequent feuds with coworkers and supervisors
- Failure to follow regulations and guidelines
- Poor attitude, including disgruntlement, temper, and false accusations
- Theft of government resources
- Substandard work performance

For these, Wells received numerous reprimands and disciplinary sanctions.

In December 2011, Wells was told by his supervisor to "be a part of the process or retire." A month later, the supervisor informed Wells that others would attend an annual conference in his stead due to his disciplinary problems. A heated discussion followed.

On April 12, 2012 Wells entered the communications rigger shop where he shot and killed two co-workers with a .44 caliber revolver. Wells murdered two Coast Guard employees, who left behind wives and children.

Subsequent FBI investigations indicated that Wells had deliberately planned the attack and attempted to establish an alibi for his actions.

Wells was found guilty of two counts of first-degree murder, two counts of murder of an officer or employee of the United States, and two counts of possession and use of a firearm in a crime of violence. He was sentenced to four consecutive life sentences and restitution of nearly $1.5 million.

So, could this horrible incident have been prevented? It is possible. If any of his ongoing negative behaviors were reported as adverse information along the way, the collection of suspicious behaviors may have come together before he was able to commit such a crime.

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 collective, 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.

Each year, DSS publishes Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting booklet which reflects the compilation and analysis of the suspicious contact reports received from cleared industry.

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 the DSS IS Rep. If warranted, the DSS IS Rep will forward your report to the DSS Counterintelligence Special Agent (CISA) for additional review. If you feel the situation is urgent, your initial report may be made by phone, but a written report must follow. Remember, it is your responsibility as the FSO to ensure cleared employees not only know of this reporting requirement but that they also understand what and how to report.

For more information on identifying suspicious contacts, refer to the *Thwarting the Enemy* Web-based training course offered by the Center for Development of Security Excellence (CDSE). You may also find the FSO Toolkit available through the CDSE Web site helpful as well.

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 academic solicitation, such as an overqualified individual seeking an intern role in a cleared environment.

The third are 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 fourth is suspicious offers to perform work for your company, such as foreign scientists, engineers, or interns offering their services for free.

The fifth is foreign contact with individuals in your company based on their family origin.

And the last is suspicious network activity. Indicators include activities like multiple attempts to unsuccessfully log into a system or accessing a system that is unrelated to the cleared employee's purview.

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

More

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 the DSS IS Rep because they are more likely to be targeting the *facility*.

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 in the sections that follow must be reported to PSMO-I via the DoD System of Record.

DoD System of Record: Currently the Joint Personnel Adjudication System (JPAS), but will soon be replaced by the Defense Information System for Security (DISS)

Change in Cleared Employee Status (NISPOM 1-302c)

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

- 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 the appropriate function in the DoD system of record.

DoD System of Record: Currently the Joint Personnel Adjudication System (JPAS), but will soon be replaced by the Defense Information System for Security (DISS)

Citizenship by Naturalization (NISPOM 1-302d)

If a non-U.S. citizen who has been granted a Limited Access Authorization (LAA) becomes a U.S. citizen through 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
- The employee's naturalization certificate number

U.S. citizenship by naturalization must be reported to PSMO-I, using the appropriate function in the current DoD System of Record.

DoD System of Record: Currently the Joint Personnel Adjudication System (JPAS), but will soon be replaced by the Defense Information System for Security (DISS)

Employees Desiring Not to Perform on Classified Work (NISPOM 1-302e)

Cleared employees at contractor facilities who express a desire not to perform classified work must be reported. If an employee at your facility no longer wishes to be processed for a security clearance or wishes to relinquish an existing clearance then you must submit a report to PSMO-I using the appropriate function in the current DoD System of Record.

DoD System of Record: Currently the Joint Personnel Adjudication System (JPAS), but will soon be replaced by the Defense Information System for Security (DISS)

Standard Form (SF) 312 (NISPOM 1-302f)

Standard Form 312 (SF-312), the Classified Information Nondisclosure Agreement, is a required part of the Personnel Security Clearance (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 appropriate function in the current DoD system of record.

DoD System of Record: Currently the Joint Personnel Adjudication System (JPAS), but will soon be replaced by the Defense Information System for Security (DISS)

Refer to Appendix C for a job aid on the reporting requirements.

Changes Affecting the Facility

Reporting on the Facility

Let's look again at the subparagraphs listed in NISPOM paragraph 1-302. These include:

- 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

In addition to the information and events impacting PCLs, contractors must also report various types of information and events that could affect the *facility's* security clearance (FCL).

The NISPOM lists different types of information or events that may affect the facility and its FCL. Recall that reports about the facility are reported in writing to the DSS IS Rep. Most reports are reported in writing, but some may be reported electronically, using the electronic Facility Security Clearance (e-FCL) system.

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? What happens if a cleared contractor facility is purchased by a foreign owner? Who actually has control and influence 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 FCL:

- Changes in company or facility ownership
- Changes in the name or address of the company or facility
- Changes to Key Management Personnel (KMPs)
- Termination of company operations for any reason, including bankruptcy
- Actual or anticipated changes in Foreign Ownership, Control, or Influence (FOCI)

Like other information affecting the facility, these change conditions are reported to your DSS IS Rep. However, these are *not* reported directly to your DSS IS Rep in writing. Instead, these changes are reported through the e-FCL system.

Key Management Personnel

The specific job titles of the KMPs in your organization will vary, but may include the following:

- Your Senior Management Official (SMO), such as the president or Chief Executive Officer, commonly referred to as the CEO
- The Vice Presidents or division directors
- The Facility Security Officer (FSO)

- Members and officers of the board of directors, including:
  - The chairman of the board
  - The secretary
  - The treasurer
  - The Insider Threat Senior Program Official (ITPSO)
  - Any stockholder in a positon to exert control and influence over the company's classified business operations

All KMPs must be listed on your KMP list but not all KMPs are required to be cleared. Generally speaking, KMPs required to be cleared in connection with your FCO include the SMO, the ITPSO, and the FSO.

Any change to the list must be reported. When reporting changes in a facility's KMPs, 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 DSS 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.

Other Changes Affecting the Facility

In addition to administrative changes about the facility, contractors must also report other circumstances affecting the FCL. Each of the facility-related reporting circumstances in the sections that follow must be reported in writing to the DSS IS Rep.

Changes in Storage Capability (NISPOM 1-302h)

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 the DSS IS Rep. Such changes may include when a company that is currently approved to store classified

material up to Secure receives a classified contract that requires safeguarding at the Top Secret level. Note that the FCL would also be required to be upgraded to the TS level.

Inability to Safeguard Classified Material (NISPOM 1-302i)

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

Security Equipment Vulnerabilities (NISPOM 1-302j)

Any significant vulnerabilities in a facility's security equipment must be reported in writing to the DSS IS Rep. This includes vulnerabilities of the Intrusion Detection Systems (IDS), access control systems, Communications Security (COMSEC) equipment or systems, and Information Systems(IS) security hardware and software.

Unauthorized Receipt of Classified Information (NISPOM 1-302k)

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 the DSS IS Rep. The report should include the following information:

- The source of the material
- Its origination
- The quantity
- The subject or title
- The date
- The classification level

Employee Information in Compromise Cases (NISPOM 1-302l)

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

Disposition of Classified Materials Terminated From Accountability (NISPOM 1-302m)

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

Foreign Classified Contracts (NISPOM 1-302n)

Contractors sometimes negotiate and award contracts outside the purview of a Government Contracting Activity (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 DSS IS Rep.

Refer to Appendix C for a job aid on the reporting requirements.

Review Activity

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 those listed below, decide whether it should be reported to PSMO-I or to your DSS IS Rep assigned to your facility.

Select PSMO-I or DSS IS Rep for each statement. Check your answer in the Answer Key at the end of this Student Guide.

Statement 1 of 6: Adverse information

- ○ PSMO-I
- ○ DSS IS Rep

Statement 2 of 6: Suspicious contacts

- ○ PSMO-I
- ○ DSS IS Rep

Statement 3 of 6: Change in cleared employee status

- ○ PSMO-I
- ○ DSS IS Rep

Statement 4 of 6: Citizenship by naturalization

- ○ PSMO-I
- ○ DSS IS Rep

Statement 5 of 6: Unauthorized receipt of classified material

- ○ PSMO-I
- ○ DSS IS Rep

Statement 6 of 6: Employee information in compromise cases

- ○ PSMO-I
- ○ DSS IS Rep

Review Activity 2

According to NISPOM paragraph 1-302g, which of the following should be reported as a changed 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 answer 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.

Lesson 4: Security Violations and Reports to the FBI

Lesson Introduction

Objectives

In addition to reporting changes related to personnel and facility security clearances, the Facility Security Officer (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 violation and what information you must report to the FBI. You will also learn how and where to send these reports.

Here are the lesson objectives:

- Define security violation
- Describe reporting requirements when classified information may have been lost or compromised
- Recognize NISPOM reports required to be submitted to the FBI
- Identify the reporting process for security violations and national security threats

Security Violations

Overview of Security Violations and Individual Culpability

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 violation that result in the loss, compromise, or suspected compromise of classified information. A cleared employee is always responsible for incident 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.

Security Violations

The NISPOM defines a security violation as the failure to comply with the policy and procedures established by the NISPOM that reasonable could result in the loss or compromise of classified information.

Examples of security violations include but are not limited to:

- 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 proper authorization
- Using an unauthorized computer to process classified information

Be aware that this final example accounts for the majority of security 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 violation that results in the loss, compromise, or suspected compromise of classified information must be reported to the DSS IS Rep.

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.

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

Compromise

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

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. 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.

Reporting Process

When reporting actual security violations resulting in the loss, compromise, or suspected compromise of classified information, you will report directly to the DSS IS Rep. Suggested timeframes for reporting are provided here, but ultimately, the reporting deadlines will be determined by the DSS 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 the DSS IS Rep during the facility's next government Security Vulnerability Assessment (SVA).

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 son the following work day.

In preparing the final report, the FSO should use the Administrative Inquiry (AI) Job Aid for Industry (available on the Course Resources page) 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. Although it is generally not the case, it is possible that, depending on the information included in the report, the initial and/or final report may be classified.

Preliminary Inquiry

The first step in reporting security 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 the 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 becomes aware that a violation has occurred.

Initial Report

The second step in reporting security violations is to prepare an initial report. Closely following the guidance found in the AI Job Aid for Industry (available through the Course Resources page), 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 the DSS IS Rep within one business day of the preliminary inquiry.

Final Report

The third and final step in the reporting process is to prepare the final report. Once again, closely following the AI Job Aid for Industry (available through the Course Resources page), the final report should contain a comprehensive description and analysis of all circumstances that necessitated the investigation. At a minimum, the final report should contain the following information:

- A reference to the initial report
- A description of the information that was lost or compromised
  - Originating activity
  - Date of origin
  - Document title
  - Number of pages
  - Description of contents
  - Associated contract or program
  - Classification level
- The essential facts of the incident
  - Who?
  - What?
  - When?
  - Where?
  - Why?
  - How?
- Personal information about the responsible party
  - Name
  - Position
  - SSN
  - Place and date of birth
  - Date PCL or LAA granted
  - Record of prior incidents for which individual was deemed responsible, if any
- A description of how the information was first reported
  - Name of person who reported

  - Name of person receiving report
  - Date of first report
- A statement describing what action was taken to secure the material
  - What action was taken to secure material and limit any further damage after discovery?
- A description of the circumstances under which the classified information was vulnerable
  - When and how long was classified information vulnerable to unauthorized disclosure?
  - How did information become vulnerable to unauthorized disclosure?
  - Who has access during period of vulnerability?
- A list of all classified information that is lost or unaccounted for
- Specific reasons for reaching the conclusion that loss, compromise, or suspected compromise did or did not occur
  - Loss
  - Compromise
  - Suspected compromise
  - No compromise
- A statement of corrective action describing what actions have been taken to prevent recurrence of similar incidents
  - What actions have been taken to prevent similar incidents?
- A description of disciplinary action taken against the responsible individual
  - What disciplinary action, if any, was taken against the responsible individual?

Note that the inclusion of some of this information, such as the listing or all lost or unaccounted classified information, could render the final report classified.

The final report must be submitted in writing to the DSS 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 the DSS IS Rep.

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
  - Example is taking classified work home over the weekend
- If the violation involved gross negligence in the handling of classified material
  - Example is locking a classified document in a desk drawer instead of ensuring proper storage
- If the violation involved was not necessarily deliberate in nature but is part of an ongoing pattern of negligence or carelessness
  - Example is repeated failure to properly secure a security container

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 the DoD System of Record.

DoD System of Record: Currently the Joint Personnel Adjudication System (JPAS), but will soon be replaced by the Defense Information System for Security (DISS)

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.

National Security Threats

National Security Threats Definition

Security threats carry with them the potential for serious harm to our national security. But what exactly are these threats? How are they defined? And what exactly must the contractor report? 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 that may occur at their facility.

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, is 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 IS Rep assigned to your facility.

Espionage

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. History has shown that most espionage cases involve government insiders, such as the case of John Beliveau, an NCIS Special Agent who deliberately leaked names of cooperating witnesses, reports of witness interviews, and plans for future investigative activities for over 5 years.

However, there have been several notable espionage cases involving contractor personnel as well. Consider the case of Bryan Underwood, a former U.S. Msarine working as a cleared American guard at the U.S> consulate in China. After losing money in the stock market, Underwood approached China's Ministry of State Security to initiate a business arrangement. Underwood attempted to commit espionage by taking over 30 photographs of sensitive areas and documenting schematics of security upgrades.

Sabotage

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.

Consider the case of Timothy Lloyd, a computer programmer who intentionally destroyed computer files of his employer because he was upset over the loss of his job. He caused irreversible damage to the systems.

Or how about Darnell Albert El, the former director of information technology for a Virginia based company? After being fired, he used his access to delete approximately 1,000 files related to the host website for the company, causing more than $6,000 in damages. Be mindful of the damaging effects of sabotage and take proper precautions.

Terrorism

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 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.

The 2009 Fort Hood shooting was a domestic attack by a U.S. citizen who was motivated by the recent death of an al-Qaeda leader with whom he was affiliated.

And in 2013, the Boston marathon bombings that killed 3 and injured 183 were carried out by two brothers who were self-radicalized and unconnected to any outside terrorist group, yet claimed motivation by their own extremist affiliation.

Subversive Activities

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 ISIS/ISIL or FARC, 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.

Refer to Appendix C for a job aid on the reporting requirements.

Review Activity

Review Activity 1

Which of the following should be reported to the FBI?

Select all that apply. Check your answer 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 paragraph 1-304 lists the requirements for reporting individual culpability. Which of the following cleared employees do you think should be reported?

Select the appropriate response for each employee. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 4: 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.

- ○ Report
- ○ Do Not Report

Question 2 of 4: 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.

- ○ Report
- ○ Do Not Report

Question 3 of 4: 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.

- ○ Report
- ○ Do Not Report

Question 4 of 4: Jill did not properly secure her storage container four times over the past six months even though she has been repeatedly instructed on proper storage procedures.

- ○ Report
- ○ Do Not Report

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 the appropriate response for each employee. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 5: Rafael was overhead discussing classified information with a colleague during his morning coffee break in the building cafeteria.

- ○ Reportable
- ○ Not Reportable

Question 2 of 5: Nancy left classified information out on a desk in an unsecured room where uncleared individuals could see the information.

- ○ Reportable
- ○ Not Reportable

Question 3 of 5: Donna left a safe containing classified material open and unattended though there is no confirmation that any classified information was disclosed

- ○ Reportable
- ○ Not Reportable

Question 4 of 5: Shane left a GSA security container unsecured in an approved closed area.

- ○ Reportable
- ○ Not Reportable

Question 5 of 5: Richard sent classified information by e-mail from an unauthorized computer.

- ○ Reportable
- ○ Not Reportable

Lesson 5: Course Conclusion

Course Conclusion

Course Summary

As you have learned, reporting is a critical responsibility of the Facility Security Officer (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 (NISP), as well as the types of information required to be reported and the reporting mechanisms for each type of information.

Course Objectives

Congratulations! You have completed the NISP Reporting Requirements course.

You should now be able to perform all of the listed activities.

- Describe reporting requirements for National Industrial Security Program (NISP) contractors
- Identify procedures for reporting personnel and facility changes
- Recognize procedures for reporting security violations and national security threats

To receive course credit, you must take the *NISP Reporting Requirements* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

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

- ☑ Reporting suspicious contacts can lead to the capture of individuals seeking to harm national security. *(correct response)*
- ☑ Reporting adverse information about employees of cleared contractor facilities can help to safeguard classified information. *(correct response)*
- ☑ 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 service members. *(correct response)*

Feedback*: All of these are reasons that reporting certain information is important.*

Review Activity 2

Several regulatory and legal documents form the basis for the requirements to report.

Question 1 of 3: The baseline security requirements (including the requirement to report) that ensure protection of classified information by contractors

- ○ E.O. 12829
- ○ DD Form 441
- ⦿ NISPOM *(correct response)*

Feedback*: The NISPOM establishes baseline security requirements that ensure protection of classified information by contractors. These requirements include the requirement to report certain information.*

Question 2 of 3: Established the partnership between the U.S. government and private industry that is known as the National Industrial Security Program

- ⦿ E.O. 12829 *(correct response)*
- ○ DD Form 441
- ○ NISPOM

Feedback*: E.O. 12829 established the partnership between the U.S. government and private industry that is known as the National Industrial Security Program.*

Question 3 of 3: The contractual agreement in which contractors agree to maintain minimum security controls to protect classified information

- ○ E.O. 12829
- ⦿ DD Form 441 *(correct response)*
- ○ NISPOM

***Feedback**: DD Form 441 is the contractual agreement in which contractors agree to maintain minimum security controls to protect classified information in accordance with the NISPOM.*

Review Activity 3

Different types of information require reporting to different government entities.

Question 1 of 3: PSMO-I

- ○ Actual or suspected espionage, sabotage, terrorism, or subversive activities
- ⦿ Changes to personnel information *(correct response)*
- ○ Changes to facility information

***Feedback**: Changes in personnel information should be reported to Personnel Security Management Office for Industry (PSMO-I).*

Question 2 of 3: DSS IS Rep

- ○ Actual or suspected espionage, sabotage, terrorism, or subversive activities
- ○ Changes to personnel information
- ⦿ Changes to facility information *(correct response)*

***Feedback**: Changes in facility information should be reported to the DSS IS Rep.*

Question 3 of 3: FBI

- ⦿ Actual or suspected espionage, sabotage, terrorism, or subversive activities *(correct response)*
- ○ Changes to personnel information
- ○ Changes to facility information

***Feedback**: Actual or suspected espionage, sabotage, terrorism, or subversive activities should be reported to the FBI.*

Lesson 3 Review Activities

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 those listed below, decide whether it should be reported to PSMO-I or to your DSS IS Rep assigned to your facility.

Question 1 of 6: Adverse information

- ⦿ PSMO-I *(correct response)*
- ○ DSS IS Rep

***Feedback**: Adverse information is related to personnel, so it is reported to PSMO-I. (1-302a)*

Question 2 of 6: Suspicious contacts

- ○ PSMO-I
- ⦿ DSS IS Rep *(correct response)*

***Feedback**: Reporting suspicious contacts is the one type of information related to personnel that is reported to your DSS IS Rep. (1-302b)*

Question 3 of 6: Change in cleared employee status

- ⦿ PSMO-I *(correct response)*
- ○ DSS IS Rep

***Feedback**: Change in cleared employee status is related to personnel, so it is reported to PSMO-I. (1-302c)*

Question 4 of 6: Citizenship by naturalization

- ⦿ PSMO-I *(correct response)*
- ○ DSS IS Rep

***Feedback**: Citizenship by naturalization is related to personnel, so it is reported to PSMO-I. (1-302d)*

Question 5 of 6: Unauthorized receipt of classified material

- ○ PSMO-I
- ⦿ DSS IS Rep *(correct response)*

***Feedback**: Unauthorized receipt of classified material is related to the facility, so it is reported to your DSS IS Rep. (1-302k)*

Question 6 of 6: Employee information in compromise cases

- ○ PSMO-I
- ⦿ DSS IS Rep *(correct response)*

***Feedback**: Although related to an individual, compromise cases affect the facility, so this information is reported to your DSS IS Rep. (1-302l)*

Review Activity 2

According to NISPOM paragraph 1-302g, which of the following should be reported as a changed 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. *(correct response)*
- ○ The company has just won a major contract.

***Feedback**: 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. *(correct response)*
- ☑ Martin Lundberg, who currently holds an LAA, became a U.S. citizen through naturalization. *(correct response)*
- ☐ Nathan purchased a new home and moved from Virginia to Maryland.
- ☑ Walt was arrested and charged with driving under the influence. *(correct response)*
- ☐ Janet received a request for classified information from an uncleared person she met at a conference.

***Feedback**: Dana was an authorized recipient of classified material, which must be reported to the DSS IS Rep. (NISPOM 1-302k). Helen's name change should be reported to PSMO-I. (NISPOM 1-302c). Martin became a citizen by naturalization, which must be reported to PSMO-I. (1-302d). Nathan's change in personal residence does not need to be reported. Walt's abuse of alcohol shows questionable judgment and is considered adverse information, which should be reported to PSMO-I. (NISPOM 1-302a). Janet has received a suspicious contact, which must be reported to the DSS IS Rep. (NISPOM 1-302b).*

Lesson 4 Review Activities

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. *(correct response)*
- ☑ A safe containing classified information appears to have been tampered with. *(correct response)*
- ☐ 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. *(correct response)*

***Feedback**: You have inconclusive evidence that an employee may have sold classified materials to alleviate his financial stress, a safe containing classified infomraiton appears to have been tampered with, and 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 are allsituations that represent actual, probable, or possible cases of espionage, sabotage, or terrorism, which must be reported to the FBI. You must also report cases of subversive activity. (NISPOM paragraph 1-301)*

Review Activity 2

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

Question 1 of 4: 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.

- ⊙ Report *(correct response)*
- ○ Do Not Report

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

Question 2 of 4: 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.

- ⊙ Report *(correct response)*
- ○ Do Not Report

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

Question 3 of 4: 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.

- ○ Report
- ⊙ Do Not Report *(correct response)*

***Feedback**: 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.*

Question 4 of 4: Jill did not properly secure her storage container four times over the past six months even though she has been repeatedly instructed on proper storage procedures.

- ⊙ Report *(correct response)*
- ○ Do Not Report

***Feedback**: 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?

Question 1 of 5: Rafael was overhead discussing classified information with a colleague during his morning coffee break in the building cafeteria.

- ⊙ Reportable *(correct response)*
- ○ Not Reportable

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

Question 2 of 5: Nancy left classified information out on a desk in an unsecured room where uncleared individuals could see the information.

- ⦿ Reportable *(correct response)*
- ○ Not Reportable

***Feedback**: 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.*

Question 3 of 5: Donna left a safe containing classified material open and unattended though there is no confirmation that any classified information was disclosed.

- ⦿ Reportable *(correct response)*
- ○ Not Reportable

***Feedback**: 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.*

Question 4 of 5: Shane left a GSA security container unsecured in an approved closed area.

- ○ Reportable
- ⦿ Not Reportable *(correct response)*

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

Question 5 of 5: Richard sent classified information by e-mail from an unauthorized computer.

- ⦿ Reportable *(correct response)*
- ○ Not Reportable

***Feedback**: Sending classified information by encrypted e-mail or over an unapproved LAN or WAN is always considered a loss and should be reported.*

Appendix B: NISP Reporting Structure Job Aid

The NISPOM

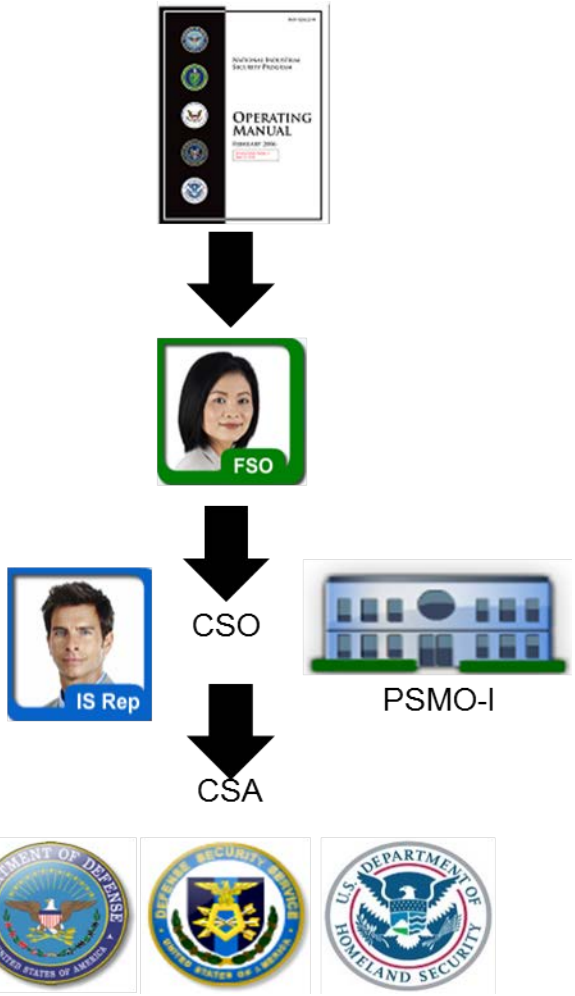
- Prescribes reporting requirements

The FSO:

- Administers their company's security program
- Educates cleared employees on their reporting responsibilities
- Receives reports from cleared employees
- Submits NISPOM required reports to the government (either their CSA or the FBI)

The CSO:

- Administers the NISP on behalf of the CSA (DSS has been delegated as the CSO for DoD and DHS)
- Receives reports on behalf of the CSA from industry
- Reports submitted to DSS are either sent to the DSS IS Rep or PSMO-I The DSS IS Rep receives reports affecting facility clearances, safeguarding, and other issues and will forward reports to other DSS entities such as the CISA or ISSP when necessary
- PSMO-I receives reports affecting personnel security clearances



The CSA:

- Maintains security cognizance over the NISP
- Includes the following agencies:
  - Department of Defense (DoD)
  - Department of Energy (DoE)
  - Nuclear Regulatory Agency (NRA)
  - Director of National Intelligence (DNI)
  - Department of Homeland Security (DHS)

Appendix C: FSO Reports To Job Aid

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 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 the DSS IS Rep in the next facility Security Vulnerability Assessment (SVA).	• Initial Report (in writing) • Final Report (in writing)	CSA (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 Reporting using appropriate function in the DoD System of Record Report should include— • Statement of the administrative actions against the employee • Details of the incident(s)	CSA (PSMO-I)