NISP Reporting Requirements

Student Guide

June 2022

Center for Development of Security Excellence

Table of Contents

Course Introduction

Course Information

Welcome to the NISP Reporting Requirements course.

Course Overview

The National Industrial Security Program, or NISP, is a government-industry partnership that was forged to ensure the protection of classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States, or U.S. agencies. One method used to ensure this protection is through the reporting requirements identified within 32 CFR part 117, National Industrial Security Operating Manual, or NISPOM, the Security Executive Agent Directive 3, or SEAD 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position, and Cognizant Security Agency, or CSA, provided guidance.

These reporting requirements pose many challenges to the Facility Security Officer, or 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. Take a moment to review them.

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 Menu

- 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

Understanding Reporting in the NISP

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 Robert 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.

Lesson Introduction

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. Take a moment to review them.

Understanding Reporting in the NISP 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, 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 developed by contractors, to prevent unauthorized disclosure. When your company signed the Department of Defense, or DOD, Security Agreement, or DD Form 441, it agreed to provide and maintain a system of security controls in accordance with requirements of the National Industrial Security Program Operating Manual, or NISPOM, and any revisions thereto required by the demands of national security as determined by the Government.

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 the NISPOM, states that contractors must report certain events to the appropriate government agencies, that may have an effect on the status of the entity's or an employee's eligibility for access to classified information. This requirement includes both your own observations and those of your cleared employees.

This requirement to report applies to certain events that may have an effect on the status of the contractor’s favorable entity eligibility determination, also referred to as a Facility Security Clearance, or FCL or affect the status of an employee’s favorable national security eligibility determination, also referred to as a Personnel Security Clearance, or PCL; may indicate an insider threat to classified information or to employees with access to classified information; affect the proper safeguarding of classified information, and indicate that classified information has been, or is suspected to be, 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 and uncleared 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 most reports will be submitted.

According to the NISPOM, most reports are submitted to the Federal Bureau of Investigation, or FBI, or the Cognizant Security Agency, or CSA. The CSA reports are submitted to the Defense Counterintelligence and Security Agency, or DCSA via the DOD personnel security system of record, with certain reports going to your DCSA Industrial Security Representative, or IS Rep. We will discuss this in greater detail later in this course.

Reporting Methods

Structure of 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, or CSO, to administer the NISP on its behalf. DCSA is delegated as the CSO for the DOD.

On the industry side, each cleared contractor facility must appoint an FSO, who supervises and directs security measures for implementing applicable NISPOM and related government security requirements to ensure the protection of classified information. One of the FSO's responsibilities is to ensure that 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 accordingly.

For the purposes of this course, we will focus on the reporting structure and processes as they apply specifically to the DOD, or CSA. The majority of NISPOM reports will be submitted to the DCSA, acting as the CSO on behalf of your CSA. Depending on the type of information that is being reported, CSA reports should be submitted to DCSA in one of two ways.

Reports that have an effect on the status of your company's FCL and safeguarding capability are submitted to the DCSA IS Rep assigned to your facility.

Reports that may have an effect on the status of the PCLs of your cleared employees are submitted to DCSA via the DOD personnel security system of record.

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, NISPOM reports designated to be sent to the CSA are submitted to DCSA. The type of information being reported will determine where the report should be sent.

Reports affecting PCLs are submitted to DCSA via the DOD personnel security system of record while reports affecting your FCL or safeguarding capabilities are submitted to the DCSA IS Rep. Depending on the nature of the report, the DCSA IS Rep may further disseminate the report to other DCSA personnel such as the Counterintelligence Special Agent or CISA and the Information System Security Professional/Security Control Assessor, or ISSP/SCA.

And finally, reports involving actual, probable or possible espionage, sabotage, terrorism, or subversive activities must be submitted to the FBI, with a copy sent to your DCSA IS Rep.

DOD Personnel Security System of Record

Reports that may affect the status of cleared personnel are submitted to DCSA using the DOD personnel security system of record.

Term:
DOD Personnel Security System of Record: A system of record for personnel security, adjudication determination, clearance, verification, and history. The term applies not only to this system but to any successor of the DOD personnel security system of record.

DCSA IS Rep

Reports that may affect the status of your company's FCL and events that affect proper safeguarding of classified information are sent to the DCSA IS Rep. These reports are submitted either in writing, by letter or e-mail, directly to the DCSA IS Rep or through the FCL System of Record.

Term:
FCL System of Record: An electronic system that is a repository of information about DOD cleared contractor facilities. The system has internal users (with full access) such as DCSA personnel and external users (with limited access). It offers a variety of functionality that facilitates the process for FCL requests, processing, and maintenance. Functions and features include but are not limited to the following: request an FCL, report a change condition, message your IS Rep, request a facility profile update, submit an FCL verification and submit an annual self-inspection certification.

FBI

Although you will submit the majority of your reports to DCSA as the CSA, some potentially grave threats to national security require immediate reporting directly to the FBI. Such threats include any information involving actual, probable or possible 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 DCSA IS Rep a copy of the report submitted to the FBI. See Lesson 4 for additional details.

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.
□ Failing to report attempts by unauthorized individuals to access classified information can lead to loss of intellectual property, thus resulting in a loss to the company's competitive advantage.
□ Reporting adverse information about employees of cleared contractor facilities can help to safeguard classified information.

Review Activity 2

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

Select the appropriate document for each statement:

Statements:

- The baseline security 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
- An agreement to provide and maintain a system of security controls in accordance with national industrial security requirements and any revisions thereto required by the demands of national security as determined by the Government

Documents:

- E.O 12829
- DD Form 441
- NISPOM

Review Activity 3

Different types of information require reporting to different government entities.
Match the Entity to the Type of Information.

Entity:

- DOD Personnel System of Record
- DCSA IS Rep
- FBI

Type of Information:

- Involving actual, probable, or possible espionage, sabotage, terrorism, or subversive activities (FBI)
- Reports affecting the status of cleared personnel (DOD Personnel Security System of Record)
- Reports affecting the status of a company's FCL (DCSA IS Rep)

Summary

You have completed the Understanding Reporting in the NISP lesson.

Lesson 3: Reporting Personnel and Facility Changes

Lesson Introduction

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 events require reporting and how each is to be reported. Here are the lesson objectives. Take a moment to review them.

Reporting Personnel and Facility Changes 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

The NISPOM identifies the various types of personnel and facility-related information and events that must be reported to the Cognizant Security Agency, or CSA.

Reports to be Submitted to the CSA:

- Adverse Information
- Suspicious Contacts
- Change in Cleared Employee Status
- Citizenship by Naturalization
- Employees Desiring Not to be Processed for a PCL or Not to Perform on Classified Work
- Refusal to Sign Standard Form (SF) 312
- Changed Conditions Affecting the Facility Clearance
- Changes in Storage Capability
- Inability to Safeguard Classified Material
- Unsatisfactory Conditions of a Prime or Subcontractors
- Dispositioned Material Previously Terminated
- Foreign Classified Contracts
- Improper Receipt of Foreign Government Material
- Reporting by Subcontractor
- Loss, Compromise or Suspected Compromise
- Employee Information in Compromise Cases
- Individual Culpability Reports
- Cyber Incident Reports

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 DCSA, using the appropriate function in the DOD personnel security system of record.

Reports about the facility, including any changes in the company's Key Management Personnel, or KMPs, are made to the DCSA IS Rep assigned to the facility. These reports are submitted either in writing directly to the DCSA IS Rep or through the FCL System of Record.

Terms:
DOD Personnel Security System of Record: A system of record for personnel security, adjudication determination, clearance, verification, and history. The term applies not only to this system but to any successor of the DOD personnel security system of record.
NISPOM: National Industrial Security Program Operating Manual

Changes Affecting Personnel

Reporting on People

Of the various reporting requirements identified in the NISPOM, 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 DCSA via the appropriate function in the DOD personnel security system of record.

The six reportable Personnel items from the NISPOM:

- Adverse Information
- Suspicious Contacts
- Change in Cleared Employee Status
- Citizenship by Naturalization
- Employees Desiring Not to be Processed for a PCL or Not to Perform on Classified Work
- Refusal to Sign Standard Form (SF) 312

The one exception is reports about suspicious contacts, which are reported to the DCSA IS Rep.
Let's look at each of these in closer detail.

Terms:
DCSA: Defense Counterintelligence and Security Agency
DOD Personnel Security System of Record: A system of record for personnel security, adjudication determination, clearance, verification, and history. The term applies not only to this system, but to any successor of the DOD personnel security system of record.
NISPOM: National Industrial Security Program Operating Manual

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 a potential or actual insider threat. It is important and required that you not only have a system in place to report adverse information using the appropriate function in the DOD personnel security system of record, but that your employees understand what is meant by the term adverse information, indicative types of this behavior and how to report it. Specific reporting requirements can be found on the course resources 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 SEAD 4, National Security Adjudicative Guidelines.

The NISPOM 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 DCSA, using the appropriate function for incident reporting in the DOD personnel security system of record. Note that you should report only credible information. 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 PCL.

Terms:
NISPOM: National Industrial Security Operating Manual.
Reporting adverse information: Contractors shall report adverse information…concerning any of their employees determined to be eligible for access to classified information
DOD Personnel Security System of Record: A system of record for personnel security, adjudication determination, clearance, verification, and history. The term applies not only to this system but to any successor of the DOD personnel security system of record.

National Security Adjudicative Guidelines Popup

The FSO should be familiar with the National Security Adjudicative Guidelines contained in SEAD-4, because it establishes the criteria for individuals who require initial or continued eligibility for access to classified information. These factors include discussion of each of the categories you see here.

National Security Adjudicative Guidelines:

- 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 investigation 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 the NISPOM, contractors must report information pertaining to suspicious contacts with employees determined to be eligible for access to classified information, and pertaining to efforts to obtain illegal or unauthorized access to the contractor's cleared facility by any means, including: Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information, Efforts by any individual to elicit information from a cleared employee, and any contact which suggests the employee may be the target of an attempted exploitation by an intelligence service of another country. 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 behavior that are much more pervasive than they may first appear.

Each year, DCSA publishes Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry, 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 DCSA IS Rep. If warranted, the DCSA IS Rep will forward your report to the DCSA Counterintelligence Special Agent, or 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 e-Learning course, Thwarting the Enemy: Providing Counterintelligence and Threat Awareness to the Defense Industrial Base offered by the Center for Development of Security Excellence, or 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.

Suspicious Indicators:

- Unsolicited requests for information
- Academic solicitation
- Inappropriate conduct during office visits
- Suspicious work offers
- Targeting cultural commonalities
- Suspicious network activity

More

Reporting suspicious contacts is an exception to the general rule about reporting personnel issues to DCSA via the DOD personnel security system of record. Though often related to people, suspicious contacts are reported to the DCSA 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 a cleared employee's status.
Each of these personnel-related reporting circumstances must be reported to DCSA via the DOD personnel security system of record.

Reports to be Submitted to the CSA

- Adverse Information
- Suspicious Contacts,
- Change in Cleared Employee Status,
- Citizenship by Naturalization,
- Employees Desiring Not to be Processed for a PCL or Not to Perform on Classified Work, and
- Refusal to Sign Standard Form (SF) 312

Term:
DOD Personnel Security System of Record: A system of record for personnel security, adjudication determination, clearance, verification, and history. The term applies not only to this system but to any successor of the DOD personnel security system of record.

Change in Cleared Employee Status

The NISPOM 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 termination of a cleared employee from the company and the change in citizenship status of a cleared employee. All changes in a cleared employee's status must be reported to DCSA, using the appropriate function in The DOD personnel security system of record.

Citizen by Naturalization

If a non-U.S. citizen who has been granted a Limited Access Authorization, or 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, and the employee's naturalization certificate number. U.S. citizenship by naturalization must be reported to DCSA, using the appropriate function in the current DOD personnel security system of record.

Terms:
DOD Personnel Security System of Record: A system of record for personnel security, adjudication determination, clearance, verification, and history. The term applies not only to this system, but to any successor of the DOD personnel security system of record.
LAA: Limited Access Authorization

Employees Desiring Not to Perform on Classified Work

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 DCSA using the appropriate function in the current DOD personnel security system of record.

Report employees desiring not to be processed for a PCL or not to perform on classified work

- Employees wishes not to perform on classified work
- Employees wishes not to be processed for a PCL or continue having a PCL

Standard Form (SF) 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 DCSA using the appropriate function in the current DOD personnel security system of record.

Terms:
DOD Personnel Security System of Record: A system of record for personnel security, adjudication determination, clearance, verification, and history. The term applies not only to this system, but to any successor of the DOD personnel security system of record.
SF 312: Classified Information Nondisclosure Agreement

Changes Affecting the Facility

Reporting on the Facility

Let’s look again at the reports listed in NISPOM to be submitted to the CSA. 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, or 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 DCSA IS Rep. Most are reported in writing, but some may be reported electronically, using the FCL System of Record. Let’s look at some of these in closer detail.

Reports to be submitted to the CSA:

- Changed Conditions Affecting the Facility Clearance
- Changes in Storage Capability
- Inability to Safeguard Classified Material
- Unsatisfactory Conditions of a Prime or Subcontractors
- Dispositioned Material Previously Terminated
- Foreign Classified Contracts
- Improper Receipt of Foreign Government Material
- Reporting by Subcontractor
- Loss, Compromise or Suspected Compromise
- Employee Information in Compromise Cases
- Individual Culpability Reports
- Cyber Incident Reports

Term:
FCL System of Record: An electronic system that is a repository of information about DOD cleared contractor facilities. The system has internal users (with full access) such as DCSA personnel and external users (with limited access). It offers a variety of functionality that facilitates the process for FCL requests, processing, and maintenance. Functions and features include but are not limited to the following: request an FCL, report a change condition, message your IS Rep, request a facility profile update, submit an FCL verification and submit an annual self-inspection certification.

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.

The NISPOM requires contractors to report the following changed conditions that affect the contractor's eligibility for access to classified information and certain events that affect the status of the FCL: 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, and actual or anticipated changes in Foreign Ownership, Control, or Influence, or FOCI.

Like other information affecting the facility, these changed conditions are reported to your DCSA IS Rep. However, these are not reported directly to your DCSA IS Rep in writing. Instead, these changes are reported through the FCL System of Record.

Terms:
FOCI: Foreign Ownership, Control, or Influence
FCL System of Record: An electronic system that is a repository of information about DOD cleared contractor facilities. The system has internal users (with full access) such as DCSA personnel and external users (with limited access). It offers a variety of functionality that facilitates the process for FCL requests, processing, and maintenance. Functions and features include but are not limited to the following: request an FCL, report a change condition, message your IS Rep, request a facility profile update, submit an FCL verification and submit an annual self-inspection certification.

Key Management Personnel

The specific job titles of the KMPs in your organization will vary, but may include the following: your Senior Management Official, or 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, or 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, or ITPSO; and any stockholder in a position 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 FCL include the SMO the ITPSO, and the FSO.
Any changes 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, and citizenship, whether they have been excluded from classified access, and whether they have been temporarily excluded from classified access while their clearance is pending.

It is important to note that even though changes in KMPs are reported to the DCSA IS Rep, any issues related to the personnel clearances of these KMPs should be reported to DCSA via the DOD personnel security system of record, just like they are for any other cleared employee.

Terms:
CEO: Chief Executive Officer
VP: Vice President
FSO: Facility Security Officer

Other Changes Affecting the Facility

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

Reports to be Submitted to the CSA

- Changed Conditions Affecting the Facility Clearance
- Changes in Storage Capability
- Inability to Safeguard Classified Material
- Unsatisfactory Conditions of a Prime or Subcontractors
- Improper Receipt of Foreign Government Material
- Dispositioned Material Previously Terminated
- Foreign Classified Contracts

Changes in Storage Capability

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 DCSA 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, or TS level. Note that the FCL would also be required to be upgraded to the TS level. Report changes in storage capability (NISPOM)

Inability to Safeguard Classified Material

Emergency situations that render a contractor facility incapable of protecting classified information must be reported immediately to the DCSA IS Rep. The FSO should provide details on how classified information will be protected and follow up with a written report when the situation is no longer an emergency. Report inability to safeguard classified material (NISPOM)

Unsatisfactory Conditions of a Prime or Subcontractors and Reporting by Subcontractor

Prime contractors, including subcontractors who have in turn subcontracted work, are required to report any information coming to their attention that may indicate that classified information cannot be adequately protected by a subcontractor, or other circumstances that may impact the validity of the eligibility for access to classified information of any subcontractor, and subcontractors will report the same of their prime contractor.

These reports are required in writing to the DCSA IS Rep. Additionally, subcontractors will also notify their prime contractor if they make any reports to their CSA per the NISPOM. Report unsatisfactory conditions of a prime or subcontractors. Per NISPOM, subcontractors must also notify their prime contractor if they make reports to their CSA.

Improper Receipt of Foreign Government Material

If a contractor facility receives classified material from foreign interests that is not received through U.S. Government channels, then a through U.S. Government channels, then a written report must be submitted to the DCSA 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. Report unauthorized receipt of classified material (NISPOM)

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 the DCSA IS Rep.

Specific reporting requirements regarding lost or compromised material will be covered in greater detail in the next lesson. Report employee information in compromise cases (NISPOM).

Dispositioned Material Previously Terminated

If classified material that was previously reported as lost and terminated from accountability, has been discovered and brought back into accountability, then a written report must be submitted to the DCSA IS Rep. Report dispositioned material previously terminated (NISPOM).

Foreign Classified Contracts

Contractors sometimes negotiate and award contracts outside the purview of a Government Contracting Activity, or GCA. If such pre-contract negotiations and contract awards not placed through a CSA or U.S. GCA that involves, or may involve the release or disclosure of U.S. classified information to a foreign interest or access to classified information furnished by a foreign interest, then this must be reported in writing to your DCSA IS Rep.

Review Activity 1

The NISPOM lists different types of events and information that must be reported and which may affect either the Facility or Personnel Security Clearance. Of those listed below, decide whether it may affect either the Facility Clearance Level (FCL) or Personnel Clearance Level (PCL).

Event	FCL	PCL
Adverse Information		
Change in cleared employee status (non-KMP)		
Suspicious Contact		
Citizenship by naturalization		

Changes in company ownership		
Foreign ownership, control, or influence (FOCI)		

Review Activity 2

The NISPOM identifies various methodology for reporting different types of events. Of those listed below, decide whether the report should be submitted to DCSA via the DCSA IS Rep, or to DCSA via the DOD Personnel Security System of Record. Select the method of reporting for each event.

Event	Via DCSA IS Rep	Via DOD Personnel Security System of Record
Adverse Information		
Change in cleared employee status (non-key management personnel (KMP))		
Suspicious contact		
Citizenship by naturalization		
Changes in company ownership		
Foreign ownership, control, or influence (FOCI)		

Review Activity 3

Which of the following events should be reported to DCSA via the DOD personnel security system of record?”

- □ 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.

Summary

You have completed the Reporting Personnel and Facility Changes lesson.

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, 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 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. Take a moment to review them.

Security Violations and Reports to the FBI Lesson Objectives:

- Define security violation
- Describe reporting requirements when classified information may have been lost or comprised
- 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 violations that result in the loss, compromise, or suspected compromise of classified information. 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, negligence in the handling of classified material, or a pattern of questionable judgement, irresponsibility, negligence, or carelessness, then the FSO must submit an individual culpability report. Let’s look at each of these reporting categories in closer detail.

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.

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, and 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 the NISPOM, 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 DCSA IS Rep.

Terms
NISPOM: National Industrial Security Program Operating Manual

Examples: Examples include but are not limited to

- Leaving a security container open and unattended
- Allowing unauthorized access to classified material
- Allowing unauthorized access to secure containers
- Sending classified material by unsecured fax
- Unauthorized removal of classified material from the facility
- Using an unauthorized computer to process classified information

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.

Suspected compromise
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.

Reporting Process

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

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 workday.

In preparing the final report, the FSO should use the Security Incident Job Aid to perform a thorough investigation of the security violation. The final report is generally submitted within 30 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 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 Security Incident Job Aid, 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 DCSA 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 Security Incident Job Aid for Industry, 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, the essential facts of the incident, personal information about the responsible party, a description of how the information was first reported, a statement describing what action was taken to secure the material, a description of the circumstances under which the classified information was vulnerable, 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, a statement of corrective action describing what actions have been taken to prevent recurrence of similar incidents, and a description of disciplinary action taken against the responsible individual.

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

The final report must be submitted in writing to the DCSA IS Rep upon completion of your detailed investigation. It is generally submitted within 30 days of the initial report, but the actual deadline will be determined by the DCSA IS Rep.

Terms:

Description of material involved:

- 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?
- How?

Information about 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

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?

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

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?

Individual Culpability

The NISPOM also covers individual culpability reports. According to NISPOM, 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 negligence in the handling of classified material, or if the violation involved was not necessarily deliberate in nature but reflects a recent or recurring pattern of questionable judgement, irresponsibility, 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 DCSA using the incident report function in the DOD personnel security system of record. 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 or disciplinary actions taken against an employee must be included in your report to DCSA via the DOD personnel security system of record.

Terms:
Deliberate disregard: Example: Taking classified work home over the weekend
Negligence: Example: Locking a classified document in a desk drawer instead of ensuring proper storage
Pattern of questionable judgement, irresponsibility, negligence, or carelessness: Example: Repeated failure to properly secure a security container

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. The NISPOM requires contractors to report to the FBI any known information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any of its locations. 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 a report is made to the FBI, the DCSA IS Rep must also be promptly notified and provided a copy of the written report.

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. Marine 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 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.

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 deliberately damaged.
□ 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

Select True or False for each statement

1. T F When the FSO issues a final report on the loss or compromise of classified information, the report must be unclassified.
2. T F When an FSO has reason to believe that classified information has been lost or compromised, the FSO must send the report directly to the DCSA IS Rep.
3. T F If a preliminary inquiry concludes that there was not a compromise, the FSO is not required to maintain the inquiry or findings.

Review Activity 3

The NISPOM requires contractors to report to the FBI any known information concerning which of the following?

□ Espionage
□ Sabotage
□ Terrorism
□ Subversive activities

Summary

You have completed the Security Violations and Reports to the FBI lesson.

Conclusion

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 have 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.

Lessons:

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

Course Conclusion

Congratulations. You have completed the NISP Reporting Requirements course.

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

- 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

To receive credit for this course, you must take the NISP Reporting Requirements examination.

.

Appendix A: Answer Key

Lesson 2 Review Activities

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.
- ☒ Failing to report attempts by unauthorized individuals to access classified information can lead to loss of intellectual property, thus resulting in a loss to the company's competitive advantage.
- ☒ Reporting adverse information about employees of cleared contractor facilities can help to safeguard classified information.

Review Activity 2

Several regulatory and legal documents form the basis for the requirement to report. Each description pairs with one of the documents. Select the appropriate document for each statement:

Statements:

- The baseline security requirements (including the requirement to report) that ensure protection of classified information by contractors
  ANSWER: NISPOM
- Established the partnership between the U.S. government and private industry that is known as the National Industrial Security Program
  ANSWER: E.O. 12829
- An agreement to provide and maintain a system of security controls in accordance with national industrial security requirements and any revisions thereto required by the demands of national security as determined by the Government
  ANSWER: DD Form 441

Review Activity 3

Different types of information require reporting to different government entities.

Match the Entity to the Type of Information.

Type of Information:

- Involving actual, probable, or possible espionage, sabotage, terrorism, or subversive activities
  ANSWER: FBI
- Reports affecting the status of cleared personnel
  ANSWER: DOD Personnel Security System of Record
- Reports affecting the status of a company's FCL
  ANSWER: DCSA IS Rep

.

Lesson 3 Review Activities

Review Activity 1

The NISPOM lists different types of events and information that must be reported and which may affect either the Facility or Personnel Security Clearance. Of those listed below, decide whether it may affect the Facility Clearance Level (FCL) or Personnel Clearance Level (PCL).

Event	FCL	PCL
Adverse Information		X
Change in cleared employee status (non-KMP)		X
Suspicious Contact	X	
Citizenship by naturalization		X
Changes in company ownership	X	
Foreign ownership, control, or influence (FOCI)	X	

Review Activity 2

The NISPOM identifies various methodology for reporting different types of events. Of those listed below, decide whether the report should be submitted to DCSA via the DCSA IS Rep, or to DCSA via the DOD Personnel Security System of Record. Select the method of reporting for each event.

Event	Via DCSA IS Rep	Via DOD Personnel Security System of Record
Adverse Information		X
Change in cleared employee status (non-key management personnel (KMP))		X
Suspicious contact	X	
Citizenship by naturalization		X
Changes in company ownership	X	
Foreign ownership, control, or influence (FOCI)	X	

Review Activity 3

Which of the following events should be reported to DCSA via the DOD personnel security system of record?”

☒ 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 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.
- ☒ A safe containing classified information appears to have been deliberately damaged.
- ☐ 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

Select True or False for each statement

1. The initial and/or final report may be classified depending upon the information included in the report.
   ANSWER: False
2. True: Reports regarding security violations resulting in loss, compromise or suspected compromise are reported directly to the DCSA IS Rep.
   ANSWER: True
3. False: When the preliminary inquiry concludes that there was no compromise, the FSO must complete the inquiry and file it away for review by the DCSA IS Rep during the next security review.
   ANSWER: False

Review Activity 3

The NISPOM requires contractors to report to the FBI any known information concerning which of the following?

- ☒ Subversive activities
- ☒ Espionage
- ☒ Sabotage
- ☒ Terrorism