NISP Security Violations and Administrative Inquiries

Student Guide

November 2018

Center for Development of Security Excellence

Student Guide

NISP Security Violations and Administrative Inquiries

Contents

Lesson 1

Introduction

You are already familiar with the National Industrial Security Program (NISP), the U.S. government's program to safeguard classified information entrusted to thousands of U.S. companies who work as government contractors. The NISP relies on many individuals in both industry and government, in a wide range of roles, to share the responsibility of ensuring that all classified information remains secure.

When a security violation is suspected or known, individuals within both industry and government have responsibilities to respond by reporting the violation, conducting an investigation, or supporting these processes. As someone who plays a role in industrial security, it is important for you to understand not only your own duties, but also the roles and responsibilities of other key industrial security personnel. A shared understanding of security violation investigations, the Administrative Inquiry (AI) process, and the roles and responsibilities of the key players involved, will help you do your part to protect national security.

Please note that the term for AI refers specifically to the Defense Security Service or DSS inquiry process; however, this term AI, will be used throughout this course to refer to all inquiries, regardless of who is conducting them.

Introduction to Your Role

There are several important roles within the NISP in relation to the investigation of security violations and administrative inquiries. These roles include:

- DSS Industrial Security Representatives (IS Reps)
- DSS Information Systems Security Professionals/Security Control Assessor (ISSP/SCAs)
- DSS Counterintelligence Special Agents (CISAs)
- Other DoD Security Specialists with Industrial Security responsibilities

Although these roles are distinct and have diverse responsibilities, they require a shared baseline understanding of government reviews required by the NISP. As such, this course is not tailored to any one role and applies across all of these roles.

Course Overview

This course will provide you with an overview of security violations, and the processes involved in reporting and investigating such incidents. It will also introduce you to the key roles within the NISP that have responsibility for processing reports of security violations and conducting administrative inquiries.

Here are the course objectives.

- Define security violation and identify the types of violations
- Identify the roles and responsibilities in conducting security violation investigations and administrative inquiries
- Identify the steps in security violation report processing and conducting administrative inquiries
- Conduct administrative inquiries of security violations
- Identify special considerations in conducting administrative inquiries of security violations involving accredited information systems

Lesson 2

Introduction

Objectives

In order to fulfill your industrial security responsibilities, you need to first understand and identify what a security violation is. You should also be familiar with the importance of investigating such violations and administrative inquiries and the roles and responsibilities associated with that process.

Here are the objectives for this lesson.

- Define security violations
- Identify the types of security violations
- Identify the roles and responsibilities related to conducting security violation investigations and administrative inquiries

Key Terms

Security Violations and Administrative Inquiries

According to the DoD, a security violation is a failure to comply with the policies and procedures established by the National Industrial Security Program Operating Manual (NISPOM) that reasonably could result in the loss or compromise of classified information. In cases where security violations occur involving classified information, the situation must be promptly reported and appropriately investigated. An investigation is necessary to determine if the classified information was at risk of compromise, the individual or individuals responsible for the violation, and appropriate corrective actions have been implemented to preclude a recurrence.

Note that the term Administrative Inquiry is generally used when the investigation is conducted by DSS. Any other investigation is simply referred to as a security violation investigation or action and not an administrative inquiry.

Types of Security Violations

Security violations are categorized as loss, compromise, and suspected compromise.

Type	Description
Loss	A loss involves classified information that is or was outside the custodian's control and the classified information cannot be located or its disposition cannot be determined. *NOTE: Classified information sent via unencrypted email is considered lost.* *Examples:* An engineer went to the security container to get a document he has used three times in the past month and found that the document cannot be located.
Compromise	A compromise is a confirmed disclosure of specifically identifiable classified information to specified unauthorized individual(s). *Example:* A SECRET document left on the copier machine is found by an uncleared employee.
Suspected Compromise	Proving that there was unauthorized access to the information may be difficult, but the facts in cases of "Suspected Compromise" would lead a reasonable person to conclude that unauthorized access more than likely occurred A suspected compromise occurs whenever identifiable classified information has been made available to unauthorized individual(s) who may have gained access to the information. *Example:* A cleared employee left a classified document on the table in an unclassified conference room overnight. The following morning when he realized what he had done, he went to retrieve the document and found that someone had placed it on the podium at the front of the room. Note: There were several other meetings scheduled for that conference room in the intervening time.

Roles and Responsibilities

Roles Overview

With an understanding of security violations, let's take a look at the different roles and responsibilities of those involved in the AI process. In order to succeed in *your* role in the AI process, you should understand not only your own responsibilities–you should also be aware of the functions carried out by others that participate in the process.

Roles and Responsibilities in the AI Process

The security violation investigation and Administrative Inquiry process involves a number of individuals who play a variety of roles in the process. These roles include, but are not limited to:

- Facility Security Officer (FSO)
- Information System Security Manager (ISSM)
- Industrial Security Representative (IS Rep)
- Information System Security Professional/Security Control Assessor (ISSP/SCA)
- Counterintelligence Special Agent (CISA)
- Government Contracting Activity (GCA)
- Personnel Security Management Office (PSMO)
- DoD Consolidated Adjudication Facility (DoD CAF)

FSO

When a security violation occurs, the FSO is responsible for conducting a preliminary inquiry, unless the violation involved the FSO or Key Management Personnel (KMP). If the FSO concludes that no loss, compromise, or suspected compromise occurred, the FSO is responsible for finalizing the inquiry and retaining the report of the inquiry and any attachments in company security files for review by the IS Rep during the next government review. If loss, compromise, or suspected compromise did occur, the FSO must notify the DSS IS Rep of the violation and submit the initial and final reports. If a culpable employee is identified, the FSO must also submit an Individual Culpability Report.

Term	Definition
Culpable Employee	In accordance with NISPOM 1-304, an individual may be found culpable for a security violation after violation has been determined and if one or more of the following factors are evident: • Deliberate disregard of security requirements • Gross negligence in the handlings of classified material • Not deliberate in nature but involves a pattern of negligence or carelessness

ISSM

During the course of a security violation investigation, if the violation involved an authorized information system, there are a number of actions the ISSM must take:

- Employ appropriate clean-up measures
- Interview all system users
- Identify what classified information was involved and the associated contracts/Government Contracting Activities (GCAs)
- Make an inventory of all affected memory, media, equipment, and components
- Communicate vulnerabilities to DSS and collaborate to identify appropriate containment solutions

IS Rep

The IS Rep receives the contractor's initial report for the preliminary inquiry and provides direction to the FSO. It is the IS Rep who determines if an Administrative Inquiry is needed. The IS Rep's responsibilities include:

- Receives the contractor's initial reports and provides direction to FSO
- Coordinates with other DSS personnel, as appropriate
- Provides written notification to the GCA
- Determines whether an Administrative Inquiry (AI) is needed
- Conducts AI under certain circumstances
- Reviews contractor's report and concurs or non-concurs with determination made

ISSP/SCA

When requested, the ISSP/SCA assists the IS Rep with violations involving information systems processing classified information. The ISSP/SCA's responsibilities include:

- When necessary/appropriate, provides onsite support at the facility in addressing/cleaning up violation
- Ensures appropriate clean-up measures are used by contractor
- When necessary/appropriate, participates in AIs involving authorized information systems

CISA

The CISA reviews all final AI reports and participates in the inquiry if there are any indicators of foreign involvement, espionage, sabotage, subversion, or terrorism.

GCA

The GCA receives reports of loss, compromise, or suspected compromise from the IS Rep and takes action with regard to downgrading or declassifying the information and mitigating damage to national security. The GCA conducts classification review and damage assessment and submits results to DSS.

PSMO

Together with the DoD CAF, PSMO processes security violations when individual culpability is determined. PMSO responsibilities include:

- Processes the security violation in which individual culpability has been determined
- Enters information into the Case Adjudication Tracking System (CATS) and forwards in *the DoD System of Record* to DoD CAF as appropriate for adjudication

DoD CAF

Together with the PSMO, the DoD CAF processes security violations when individual culpability is determined. DoD CAF responsibilities include:

- Prepares recommendations for suspensions of eligibility, when applicable, for all contractor personnel under the NISP
- Adjudicates the security violations processed and forwarded by PSMO

Review Activities

Review Activity 1

Contractor Stephen Winters has a SECRET clearance. He saves the classified documents he works with on a removable hard drive, which he usually stores in a GSA approved container when not in use, in accordance with security protocols. However, when he left work late yesterday afternoon, he placed the hard drive in his unlocked desk drawer rather than the GSA approved container. When he returned to work this morning, the drive was missing. Which type of security violation does this scenario illustrate?

Select the best response and then check your answer in the Answer Key at the end of this Student Guide.

- ○ Suspected Compromise
- ○ Compromise
- ○ Loss

Review Activity 2

Jane Simpson, an engineer with a SECRET clearance, sent an email over an unauthorized system to her Program Manager and copied several cleared and uncleared coworkers. When the Program Manger opened the email, she noticed the attachment was marked SECRET. Which type of security violation does this scenario illustrate?

Select the best response and then check your answer in the Answer Key at the end of this Student Guide.

- ○ Suspected Compromise
- ○ Compromise
- ○ Loss

Review Activity 3

Who is responsible for conducting the preliminary inquiry after a security violation has occurred?

Select the best response and then check your answer in the Answer Key at the end of this Student Guide.

- ○ IS Rep
- ○ ISSM
- ○ FSO
- ○ ISSP/SCA

Conclusion

Lesson Summary

This concludes the lesson “Security Violations Overview.”

Answer Key

Review Activity 1

Contractor Stephen Winters has a SECRET clearance. He saves the classified documents he works with on a removable hard drive, which he usually stores in a GSA approved container when not in use, in accordance with security protocols. However, when he left work late yesterday afternoon, he placed the hard drive in his unlocked desk drawer rather than the GSA approved container. When he returned to work this morning, the drive was missing. Which type of security violation does this scenario illustrate?

- ○ Suspected Compromise
- ○ Compromise
- ⊙ Loss (correct response)

Feedback*: A loss involves classified information that is or was outside the custodian's control and the classified information cannot be located or its disposition cannot be determined.*

Review Activity 2

Jane Simpson, an engineer with a SECRET clearance, sent an email over an unauthorized system to her Program Manager and copied several cleared and uncleared coworkers. When the Program Manger opened the email, she noticed the attachment was marked SECRET. Which type of security violation does this scenario illustrate?

- ○ Suspected Compromise
- ○ Compromise
- ⊙ Loss (correct response)

Feedback*: Since the classified data was transmitted over an unauthorized system, it is a Loss.*

Review Activity 3

Who is responsible for conducting the preliminary inquiry after a security violation has occurred?

- ○ IS Rep
- ○ ISSM
- ◉ FSO (correct response)
- ○ ISSP/SCA

***Feedback**: When a security violation occurs, the FSO is responsible for conducting a preliminary inquiry.*

Lesson 3

Introduction

Lesson Objectives

Initial reporting of security violations is essential so that security violations may be investigated and containment plans may be put into action. For the process to be effective, it is important that you understand each step of the process and the actions that are required throughout.

Here are the objectives for this lesson.

- Identify the preliminary inquiry process
- Identify requirements for an initial report
- Identify government response to an initial report

Preliminary Inquiry Process

Purpose

When a contractor facility experiences a security violation, the Facility Security Officer (FSO) conducts a preliminary inquiry to secure the classified information and gather all the facts. The FSO will determine if the classified information was subject to loss, compromise, or suspected compromise. The FSO will work with his or her Industrial Security Representative (IS Rep) to determine if the violation warrants further investigation.

Let’s take a closer look.

Preliminary Inquiry Findings

When the FSO conducts the preliminary inquiry, he or she may find evidence of possible loss, compromise or suspected compromise. If so, the FSO must document the findings and notify the Cognizant Security Agency (CSA). If the facility is located on a Government installation, the installation must also receive the report. If no loss, compromise, or suspected compromise is found, the FSO will finalize the report and maintain a copy for DSS to review during the next government review.

Initial Report Requirements

The initial report filed by the FSO requires the following information: the nature of the security violation, which includes the circumstances, relevant sections of NISPOM that were violated, who was involved, when and where it occurred, how it was discovered, and who reported it to whom. The report must also include when the

violation was reported. Was it reported immediately, and if not, why? The report must also include a listing of all classified information involved, including contract number, procurement activity (Procuring Contracting Officer (PCO)/Administrative Contracting Officer (ACO)), and point of contact information. Finally, the FSO must also include in the report the Government Contracting Activity (GCA) with cognizance over the classified information, including contact information.

DSS Response to an Initial Report

Once the initial report is complete and filed, there are a series of steps that follow leading up to a government response to the security violation incident. The IS Rep:

- Directs FSO to complete and submit final report
- Assigns a DSS violation case number
- Creates an action in Industrial Security Field Database (ISFD), or its Successor System
- Notifies DSS Regional Director and Field Offices involved
- Provides a copy of the preliminary report to:
  - Field Office Chief (FOC)
  - Local CI Special Agent (CISA)
  - Local ISSP/SCA, if applicable
- Provides written notification to the GCA's headquarters security and CI elements
- Provides any required follow-up notifications to the GCAs upon receipt of the final report

These steps can be found in more detail in the Administrative Inquiry/Security Violation Investigation Process Job Aid found in the Course Resources.

GCA Response to an Initial Report

When a security violation occurs and the investigation finds that classified information was compromised, the GCA should conduct a Classification Review to determine whether affected information should be declassified or downgraded, identify measures to protect against threat to national security, and inform DSS of the results of their review.

Who Should Conduct the AI?

When the preliminary inquiry finds that further investigation is needed, in most circumstances, the FSO should be the person to conduct the investigation. In some

situations, it may be more appropriate for the IS Rep, and not the FSO, to conduct the final or follow-on AI. Those circumstances include the following:

- The violation involves the facility's security staff or Key Management Personnel (KMP).
- The contractor FSO is unable or unwilling to conduct a thorough AI.
- The violation is of an unusually sensitive nature or of high interest.
- The GCA or Special Access Program (SAP) customer requests that DSS conduct the AI.
- The violation involves indicators of possible involvement with a foreign country, espionage, sabotage, subversion, or terrorism.

Review Activities

Introduction

Consider this. An FSO submits the following initial report.

Company ABC
Security Violation Initial Report
Prepared by William Kelley, FSO
Date: Submitted Wednesday, 10:55 AM

Summary

On Tuesday afternoon last week, Employee A accidentally left a folder containing classified documents (SECRET) on a table in an unsecured conference room in the Company ABC office. On Friday afternoon, Employee B found the folder in the conference room and reported it to FSO Kelley. FSO Kelley has conducted a preliminary inquiry. In this case of suspected compromise, we deem it unlikely that anyone used the conference room or saw the documents between Tuesday and when the documents were recovered on Friday.

Personnel Involved

- **Employee A.** Team lead, SECRET clearance, employed with Company ABC for three years. Said she was using the conference room for a project meeting where they had been reviewing the documents and probably left the folder there when she returned to her office. Feels it was an accidental oversight because she was distracted by a co-worker's request for help.
- **Employee B.** Analyst, SECRET clearance, employed with Company ABC for 1.5 years, subordinate to Employee A. Entered the conference room Friday afternoon looking for a co-worker and saw the folder. Immediately reported to FSO Kelley.
- **FSO Kelley.** Company ABC FSO, TOP SECRET clearance. Conducted interviews and prepared initial report.

Location of Violation

The Conference Room is located on the 6th floor of Company ABC's downtown office. The room is dedicated for use by Employee A's team and is seldom used. The door cannot be locked and the room is therefore technically accessible to any employees or registered guests in the office. Janitorial crews clean the room nightly as needed.

Timing of Violation

- The folder was probably left in the conference room by Employee A on Tuesday around 3:00 PM.
- Employee B saw the folder and reported it Friday at 5:15 PM.
- Preliminary investigation was conducted beginning the following Tuesday at 7:30 AM (Monday was a federal holiday).

Classified Information Involved

The folder contained two documents, under the cognizance of Defense Agency XYZ:

1. Draft specifications for a SECRET-level weapons training simulation program.
2. Full names, email addresses, assigned usernames, and temporary login passwords for a group of 10 analysts tasked to beta test the simulation.
    a. Classification: SECRET
    b. Originator: Employee A
    c. Prime Contract #: W123X456Y789Z
    d. Facility name: Company ABC
    e. CAGE code: XXXXXX
    f. Procurement Activity: Defense Agency XYZ Acquisition Branch

Employee A stated that the information is typically stored in a locked GSA-approved security container in her locked office, on the secure 6th floor of Company ABC's downtown office.

Relevant NISPOM Sections

This incident appears to be a violation of NISPOM Section 5-303, "SECRET Storage."

Review Activity 1

Which of these requirements for an initial report were NOT met by the initial report filed by FSO Kelley?

Select all that apply and then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Description of the circumstances surrounding the violation
- ☐ Relevant sections of NISPOM that were violated
- ☐ Who was involved in the violation
- ☐ Where and when the violations occurred
- ☐ How the violation was reported
- ☐ When the violation was reported after discovery
- ☐ Explanation of delay in report, if applicable
- ☐ Listing of all involved classified information
- ☐ The GCA with cognizance over the classified information

Review Activity 2

In the scenario involving the security violation at Company ABC, who should conduct further investigation of the violation?

Select the best response and then check your answer in the Answer Key at the end of this Student Guide.

- ○ FSO
- ○ IS Rep
- ○ GCA
- ○ ISSP/SCA

Conclusion

You have completed the lesson “Initial Reporting of Security Violations.”

Answer Key

Review Activity 1

Which of these requirements for an initial report were NOT met by the initial report filed by FSO Kelley?

- ☐ Description of the circumstances surrounding the violation
- ☐ Relevant sections of NISPOM that were violated
- ☐ Who was involved in the violation
- ☐ Where and when the violations occurred
- ☐ How the violation was reported
- ☐ When the violation was reported after discovery
- ☑ Explanation of delay in report, if applicable (correct response)
- ☐ Listing of all involved classified information
- ☑ The GCA with cognizance over the classified information (correct response)

Feedback: *There were two problems with FSO Kelley's Initial Report:*

1. *No explanation was provided for the delay in reporting the security violation.*
2. *While it listed the GCA with cognizance over the classified information, it did not provide contact information for a point of contact.*

Review Activity 2

In the scenario involving the security violation at Company ABC, who should conduct further investigation of the violation?

- ◉ FSO (correct response)
- ○ IS Rep
- ○ GCA
- ○ ISSP/SCA

Feedback: *The FSO should conduct the investigation or inquiry into this security violation, because the violation involved two employees of Company ABC.*

Lesson 4

Introduction

Lesson Objectives

In this lesson, you will walk through the steps of conducting an Administrative Inquiry (AI) of a security violation.

Here are the lesson objectives.

- Conduct Administrative Inquiries (AI) of security violations
  - Identify the purpose of an administrative inquiry
  - Identify the basic components of an administrative inquiry
  - Identify effective practices for conducting investigative procedures
  - Determine appropriate corrective actions
  - Determine culpability of individuals
  - Identify requirements for final report
  - Identify DSS AI
  - Determine GCA notification steps

Overview

Roles and Responsibilities

As you learned earlier in this course, the Facility Security Officer (FSO) typically conducts inquiries into security violations. Under certain circumstances, the Industrial Security Representative (IS Rep) or government security specialist may conduct the follow-on administrative inquiry based on the reported facts in the preliminary report. In addition, the Information System Security Professional/Security Control Assessor (ISSP/SCA), Counterintelligence Special Agent (CISA), and contractor Information System Security Manager (ISSM) may also assist in the inquiry process, as appropriate.

Purpose

Whether an inquiry into a security violation is conducted by an FSO or a government representative, the purpose is to determine whether a loss, compromise, or suspected compromise occurred. As part of the inquiry, it is important to establish the circumstances surrounding the violation and who was involved, identify appropriate corrective actions, and determine individual culpability, if applicable. The National Industrial Security Program Operating Manual (NISPOM) and the Administrative Inquiry/Security Violation Investigation Process Job Aid provide

guidance. The output of the inquiry is the final report which includes the circumstances that led to the violation or allegation and describe actions taken as a result. If the final report is conducted by the FSO, then it must be submitted to DSS within 15 days of discovery of the security violation.

Process Steps

Overview

There are several steps that must be followed when conducting an inquiry. First, the FSO, IS Rep, or other contractor or DSS personnel will investigate the circumstances around the security violation to determine if a loss, compromise, or suspected compromise occurred. Next, they will determine what corrective actions are needed and make a determination of culpability before submitting a final report. If the contractor submits the final report to DSS, DSS will then process the inquiry and notify the Government Contracting Activity ***(***GCA***)***.

Loss, Compromise, or Suspected Compromise?

Remember, one of the purposes of the AI process is to determine whether a Loss, Compromise, or Suspected Compromise of classified information occurred. Review the definitions here and keep these in mind as you proceed through each step in the AI process.

Type of Security Violation	Description
Loss	Classified information that is or was outside the custodian's control, AND the classified information cannot be located or its disposition cannot be determined
Compromise	A confirmed disclosure of specifically identifiable classified information to specified unauthorized individual(s)
Suspected Compromise	Identifiable classified information has been made available to unauthorized individual(s) who may have gained access to the information

Investigative Procedures

Next, the individual conducting the inquiry conducts investigative procedures to gather necessary information about the security violation. This includes conducting interviews of those involved—including relevant co-workers and management—to determine if there were any indicators of intent for security violations, or concerns regarding the individual's ability to protect classified information. If necessary, you might also have to collect written statements from the interviewees. Finally, as part of

the investigation, workspaces and any applicable accesses to computer systems, such as email, shared drives, and cellular communications, should be reviewed.

Corrective Actions

Once the investigation is complete, corrective actions are considered. The appropriate corrective actions will vary depending on the circumstances of each security violation, but generally involve notifying all facilities and personnel affected by the violation, providing additional security training to prevent future violations, and notifying and coordinating with the GCA. No matter what specific actions are taken, the goal of corrective actions is always three-fold: to secure affected information, discipline culpable individuals and prevent future violations.

Determination of Culpability

The NISPOM identifies several factors that can be used to assess the culpability of personnel involved in the security violation. If the contractor personnel involved in the security violation meet the criteria, then an Individual Culpability Report must be submitted to the Personnel Security Management Office (PSMO) via the DoD System of Record

To view additional information on how this is done, please refer to the DSS PSMO page on Incident Reports available in the Course Resources.

Final Report

When an investigation is complete, corrective actions have been taken or identified, and culpability has been determined, it's time to prepare the Final Report. The report must include a summary of the inquiry, the information used to arrive at the determination, and the reasons for the determination in accordance with specific NISPOM requirements as well as supporting documentation. In addition, the final report must include the sections listed here.

Section	Description
Authority	• The reason why the inquiry was conducted • When and where the inquiry was conducted • Who conducted the inquiry
Essential Facts	• A description of the circumstances surrounding the violation and NISPOM provisions that were violated • Who was involved, including level and type of personnel clearance of the individuals involved • When and where the violation occurred • All affected classified information

Section	Description
Corrective Actions	• Summary of the corrective actions taken by the facility • Specific actions initiated or taken by the facility to secure the information after the violation was discovered • Any disciplinary actions taken against the culpable individual(s) involved in the security violation and description of the graduated scale of disciplinary actions • Notification of and coordination with the GCA
Conclusions	• Formal determination for each security violation as previously identified (loss, compromise, suspected compromise, no compromise) • Vulnerability of classified information • Description of unauthorized access • Description of GCA Classification Review
Determination of Culpability	• Procedures followed to investigate the individual(s) involved in the security violation • Whether the violation involved: o Deliberate disregard for security requirements o Gross negligence o Pattern of negligence • The individual(s) involved in the violation o Description of individual actions o Awareness of NISPOM and associated security guidelines, policies, and provisions o Notification of PSMO
Recommendations	• Includes any recommendations that would prevent a recurrence

DSS Processing

When the Final Report is completed, the IS Rep is responsible for informing the contractor involved in the security violation and coordinating actions with other DSS entities. The following information must be reported to the contractor:

- DSS concurrence or non-concurrence with the findings of the final report
- Reasons for the DSS determination
- Advisement on the acceptability of corrective actions taken or proposed
- Verification that the contractor report has met NISPOM 1-304 “Individual Culpability Reports” requirements

Other DSS entities with which actions or information may need to be coordinated include the ISSP/SCA, CISA, FOC, and RD. If culpability is identified, then the IS

Rep will provide PSMO with a copy of the final report within five days of closure of the violation.

PSMO

The final report is submitted to PSMO in order to ensure that all appropriate actions are taken to assess the risk of an individual's continued eligibility to access classified information.

- Required in cases of individual culpability
- Provide clear factual details and any information outlined in NISPOM 1-303
- Include the statement of administrative actions taken against the employee
- Within 5 days of closure of violation

Notifying the GCA

If a determination is made that a loss, compromise, or suspected compromise has occurred, the DSS process is for the IS Rep to provide a report to the appropriate GCA identifying the information involved, the circumstances surrounding the violation, a rationale for the determination, and corrective or disciplinary action taken by the contractor. The report should indicate that the IS Rep requests a GCA classification review with regard to downgrading or declassifying the information and the mitigation of damage to national security and a copy of the classification review results. Within five days of coordination with all relevant DSS elements, the IS Rep will forward the final report to the GCA point of contact indicated on the DD Form 254, with a copy to the agency headquarters' security and counterintelligence elements. The security violation is considered closed when the final report is received from the FSO and subsequent notification of the loss, compromise, or suspected compromise is made to the GCA.

Review Activities

Scenario

You've learned the steps of the AI process. Now let's put your knowledge into action in the scenario of a security violation at Company ABC. Let's review the basics of the case: Employee A left a folder containing SECRET documents on a conference room table. The folder and the documents were found several days later and secured. Many people may have access to the unlocked conference room; however, the FSO thinks it is unlikely that anyone used the conference room or discovered the documents during the week.

Company ABC
Security Violation Initial Report
Prepared by William Kelley, FSO
Date: Submitted Wednesday, 10:55 AM

Summary

On Tuesday afternoon last week, Employee A accidentally left a folder containing classified documents (SECRET) on a table in an unsecured conference room in the Company ABC office. On Friday afternoon, Employee B found the folder in the conference room and reported it to FSO Kelley. FSO Kelley has conducted a preliminary investigation. In this case of suspected compromise, we deem it unlikely that anyone used the conference room or saw the documents between Tuesday and the recovery of the documents on Friday.

Personnel Involved

- **Employee A.** Team lead, SECRET clearance, employed with Company ABC for three years. Said she was using the conference room for a project meeting where they had been reviewing the documents and probably left the folder there when she returned to her office. Feels it was an accidental oversight because she was distracted by a co-worker's request for help.
- **Employee B.** Analyst, SECRET clearance, employed with Company ABC for 1.5 years, subordinate to Employee A. Entered the conference room Friday afternoon looking for a co-worker and saw the folder. Immediately reported to FSO Kelley.
- **FSO Kelley.** Company ABC FSO, TOP SECRET clearance. Conducted interviews and prepared initial report.

Location of Violation

The Conference Room is located on the 6th floor of Company ABC's downtown office. The room is dedicated for use by Employee A's team and is seldom used. The door cannot be locked and the room is therefore technically accessible to any employees or registered guests in the office. Janitorial crews clean the room nightly as needed.

Timing of Violation

- The folder was probably left in the conference room by Employee A on Tuesday around 3:00 PM.
- Employee B saw the folder and reported it Friday at 5:15 PM.
- Preliminary investigation was conducted beginning the following Tuesday at 7:30 AM (Monday was a federal holiday).

Classified Information Involved

The folder contained two documents, under the cognizance of Defense Agency XYZ:

1. Draft specifications for a SECRET-level weapons training simulation program.
2. Full names, email addresses, assigned usernames, and temporary login passwords for a group of 10 analysts tasked to beta test the simulation.
    a. Classification: SECRET
    b. Originator: Employee A
    c. Prime Contract #: W123X456Y789Z
    d. Facility name: Company ABC
        i. CAGE code: XXXXXX
    e. Procurement Activity: Defense Agency XYZ Acquisition Branch
        i. COR: A. Smithson; email: asmithson@defenseagencyxyz.mil; phone: 555-123-4567

Employee A stated that the information is typically stored in a locked GSA-approved security container in her locked office, on the secure 6th floor of Company ABC's downtown office.

Relevant NISPOM Sections

This incident appears to be a violation of NISPOM Section 5-303, “SECRET Storage.”

Employee A

“I’m pretty sure I left the folder on the conference room table Tuesday afternoon around 3:00. I was in there for a project meeting from 2:00-3:00 PM. Employee B was with me too. When the meeting was over, Samantha from another team came in to ask me a question and I guess I just got distracted and left the folder there. Then I had to rush to the airport for a short work trip. I’m not normally so forgetful. I normally keep all these files in a locked GSA-approved security container inside my locked office.”

Employee B

“I walked into the conference room Friday afternoon and I saw the folder. I immediately recognized it from our project meeting on Tuesday – we had been reviewing the documents. I knew Employee A was out of the office so I called the FSO right away. I’m not too surprised because she leaves papers everywhere. But honestly, I doubt anybody went in the conference room all week. That conference room is dedicated for our team.”

FSO

“I received the call from Employee B around 5:15 on Friday. I immediately went to the 6th floor, obtained and secured the documents, and checked for any signs of tampering or disturbance. The documents looked untouched and it seemed like the room had been empty all week. I interviewed Employee B and left a voicemail for Employee A. Tuesday morning when we all got back to the office I interviewed Employee A and gathered the other information for the Initial Report. I finished and submitted it Wednesday morning.”

Employee A’s Supervisor

“I’m disappointed to hear about this. Employee A has done a great job leading this project. Nobody understands it like her. However, she has failed to follow procedures before. This is her first time on a SECRET-level project, so we’ve had a couple refreshers on security best practices to make sure the whole team handles the information appropriately.”

Review Activity 1

After reviewing the facts of the case, select the best answer for each question below and then check your answers in the Answer Key at the end of this Student Guide.

Did the violation involve a deliberate disregard for established requirements?

- ○ Yes
- ○ No

Did the violation involve gross negligence in the handling of classified information?

- ○ Yes
- ○ No

Was the violation deliberate in nature?

- ○ Yes
- ○ No

If the violation was not deliberate, does the individual(s) exhibit a pattern of negligence and/or carelessness in the handling of classified information?

- ○ Yes
- ○ No

Review Activity 2

After reviewing the facts of the case, select the best answer for each question below and then check your answers in the Answer Key at the end of this Student Guide.

Should the FSO submit a NISPOM 1-304 Individual Culpability Report for Employee A?

- ○ Yes
- ○ No

Must the IS Rep conduct the administrative inquiry?

- ○ Yes
- ○ No

Should the IS Rep concur with the contractor's conclusion of suspected compromise?

- ○ Yes
- ○ No

Is a final report required?

- ○ Yes
- ○ No

Review Activity 3

After reviewing the facts of the case, select all that apply and then check your answer in the Answer Key at the end of this Student Guide.

Which of the following are appropriate corrective actions in this situation?

- ☐ Notify and coordinate with GCA
- ☐ Notify PSMO of individual culpability
- ☐ Suspend Employee A's access to classified information
- ☐ Provide remedial security training

Scenario Wrap-Up

The inquiry process for the security violation at Company ABC resulted in a conclusion of suspected compromise but did not reveal a pattern of negligence or carelessness in the way Employee A handled classified information. DSS recommended remedial security training for the team and a formal warning for Employee A.

Conclusion

Lesson Summary

You have completed the lesson “Administrative Inquiry Process.”

Answer Key

Review Activity 1

Did the violation involve a deliberate disregard for established requirements?

- ○ Yes
- ⊙ No (correct response)

Feedback: *Employee A did not demonstrate deliberate disregard for established requirements.*

Did the violation involve gross negligence in the handling of classified information?

- ○ Yes
- ⊙ No (correct response)

Feedback: *Employee A did not demonstrate gross negligence in the handling of classified information.*

Was the violation deliberate in nature?

- ○ Yes
- ⊙ No (correct response)

Feedback: *Employee A did not demonstrate deliberate intention of violating security guidelines.*

If the violation was not deliberate, does the individual(s) exhibit a pattern of negligence and/or carelessness in the handling of classified information?

- ○ Yes
- ⊙ No (correct response)

Feedback: *Your investigation revealed that she has demonstrated a pattern of negligence or carelessness in handling papers, but no evidence that she has been negligent or careless in the handling of classified information.*

Review Activity 2

Should the FSO submit a NISPOM 1-304 Individual Culpability Report for Employee A?

- ○ Yes
- ⊙ No (correct response)

Feedback: *Although Employee A was responsible for the security violation, the NISPOM 1-304 criteria for individual culpability were not met.*

Must the IS Rep conduct the administrative inquiry?

- ○ Yes
- ⊙ No (correct response)

Feedback: *None of the circumstances surrounding the security violation require the IS Rep to conduct the administrative inquiry.*

Should the IS Rep concur with the contractor's conclusion of suspected compromise?

- ⊙ Yes (correct response)
- ○ No

Feedback: *Although unauthorized access to the classified information was not confirmed, it was left in a location where unauthorized individual(s) could have gained access.*

Is a final report required?

- ⊙ Yes (correct response)
- ○ No

Feedback: *A final report is required in all cases of loss, compromise, or suspected compromise.*

Review Activity 3

Which of the following are appropriate corrective actions in this situation?

- ☑ Notify and coordinate with GCA (correct response)
- ☐ Notify PSMO of individual culpability
- ☐ Suspend Employee A's access to classified information
- ☑ Provide remedial security training (correct response)

Feedback: *Because a suspected compromise occurred, the contractor and DSS must notify and coordinate with the GCA in response to the violation. In this case, individual culpability was not established, so PSMO does not need to be notified. The employee's actions do not warrant suspending access to classified information, but the contractor should provide remedial security training to prevent future violations.*

Lesson 5

Introduction

Objectives

In a world driven by technology, it can be expected that there will be incidents of security violations involving Information Systems (IS). It is important to know what considerations need to be made when addressing security violations involving authorized IS.

Here are the objectives for this lesson.

- Recognize types of Information System (IS) Security Violations
- Identify components of an Incident Response (IR) Plan
- Identify additional requirements and activities for violations involving IS
- Identify special consideration for security violations involving unauthorized systems
- Recognize when Information System Security Professional/Security Control Assessor (ISSP/SCA) involvement is required for security violations involving IS

What is an IS Security Violation?

Overview of IS Security Violations

Now that you are acquainted with the general inquiry process for security violations, let's address the specific requirements related to security violations involving ISs. While there are many similarities in the process, there are some specific differences involving risks, challenges, and required actions, of which security personnel should be aware.

As an overview of IS Security Violations, it is important to note that security violations can involve both authorized and unauthorized ISs and various personnel have specific roles and responsibilities in IS security violations. Note that in addition to the roles you are already familiar with, the DSS National Industrial Security Program Authorization Office, or NAO, and the owner of the data affected by the security violation also play important roles.

When a security violation does occur, it is essential to contain the damage and mitigate the violation, determine the extent and scope of the security incident, and document the incident. Additional guidance can be found in the DSS Assessment and Authorization Process Manual or DAAPM.

Types of IS Security Violations

Let's first take a look at the different types of IS security violations.

Unauthorized Access

When a system or information on the system is accessed by unauthorized individuals.

Investigations into violations involving unauthorized access should:

- Include a description of how the access was achieved
- Provide, as completely as possible, identification data regarding the unauthorized individual(s)

Data Spills

- Occur when classified information is introduced to an unclassified computer system or to a computer system authorized at a lower classification level than the data being entered
- May occur either by someone within the company originating the offending file(s) or when someone within the company receives the offending file(s)
- Examples of situations that can result in data spills include:
  - Emails
  - Mismarked files on servers
  - Improperly marked hard copies or media

Processing Classified Info on Unauthorized Systems

When classified information is being processed on an unauthorized system

- May occur when an authorized system is no longer authorized and the processing of classified information continues
- The Facility Security Officer (FSO), Information System Security Manager (ISSM) and Information System Security Professional/Security Control Assessor (ISSP/SCA)have the responsibility to identify when systems are no longer authorized to process classified information

Failure to Report Suspicious Contacts

A suspicious contact is any attempt to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. While a suspicious contact is not a security violation, failure to report the contact to the appropriate government entity is a security violation.

How to prevent suspicious contacts:

- Identify who might want to obtain your technology
- Identify the primary methods an adversary might utilize to obtain your technology
    - Surveillance may be one method of operation used by an illicit collector of defense information.
- Security violations and administrative inquiries are often viewed as an internal mistake; however, they can be indicative of something else going on. If so, it may be a suspicious contact.
- If you receive a suspicious email follow the proper procedures to report it. Don't assume the email is nothing.

Inadvertent Exposure

- Contractors must not download documents that are known or suspected to contain classified information.
- Classified information, even if already exposed to the public domain, remains classified and must be treated as such until declassified be appropriate authorities.
- Contractors who inadvertently discover potentially classified information in the public domain shall report its existence immediately to their FSO and delete information according to provided procedures.
- NOTE: Administrative inquiries and adverse reports are not required in the case of inadvertent exposure.
- Inadvertent Access guidance can be found within the Course Resources.

Review Activity 1

Contractor Julie Williams has a CONFIDENTIAL clearance. While working on a specific assignment and conducting internet research using her work computer, she downloads a file that appears to be relevant to her assignment. As she reads through the document, she quickly realizes that the document contains SECRET information that should not be available to the public.

Which type of IS security violation does this scenario illustrate?

Select the best response and then check your answer in the Answer Key at the end of this Student Guide.

- ○ Unauthorized Access
- ○ Data Spills
- ○ Processing Classified Info on Unauthorized System
- ○ Suspicious Contacts
- ○ Inadvertent Exposure

Review Activity 2

Employee Jeremy Wallace's computer has some issues and glitches that are being addressed by the company's Information Technology specialists. While his computer is unavailable, he's been using a nearby shared work station. A few hours later, it is brought to Jeremy's attention that the shared work station had not been authorized to process the types of classified information he had been working with.

Which type of IS security violation does this scenario illustrate?

Select the best response and then check your answer in the Answer Key at the end of this Student Guide.

- ○ Unauthorized Access
- ○ Data Spills
- ○ Suspicious Contacts
- ○ Inadvertent Exposure

Incident Response (IR) Plans

Purpose

To mitigate violations should they occur, contractors with authorized ISs should have an Incident Response (IR) plan in place.

The purpose of an IR Plan is to

- Provide a roadmap for implementing response capability
- Describe the structure of response capability
- Provide a high-level approach for how the IR fits into the overall organization
- Define reportable incidents
- Provide metrics for measuring capability
- Define resources and management support needed to maintain and mature the IR capability

The plan should meet the unique requirements of the organization, in terms of mission, size, and structure, and should be reviewed and approved by designated officials.

Procedures

Let’s take a closer look at the components of the IR Plan and the specific response procedures. To quickly respond to security violations should they occur, the IR Plan should contain points of contact, notification requirements, and cleanup procedures. The contractor should coordinate with the Government Contracting Activity (GCA) or data owner to obtain their cleanup procedures for data spills. Specific response procedures may include stopping all processes, quarantining the location of classified information, creating event logs and back-up databases, and activating standard reporting vehicles. The guidelines for cleanup should be implemented as soon as possible to avoid further contamination.

Copies of the IR Plan should be distributed to appropriate incident response personnel. The plan is reviewed and revised on an ongoing basis to ensure accuracy to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

See the AI Guidelines for Information Systems and the DAAPM available from the course resources, for more information.

Response Procedure	Description
Stop all processes	This will limit system interruption and the impact to other users of the system(s). It may include erasing/wiping of files, folders, and drives and should encompass all applications and media with access to the associated system(s).
Quarantine classified information	The plan should define the quarantine location for classified information during investigation and classification review. If available, the quarantine location should be a GSA-approved container or approved Closed Area.
Create event logs and back-up databases	The plan should address the: • Location and retrieval methods for IS Event Log(s) and back-up databases for evaluation • Restoration of records, files, and/or applications The Event Log can provide additional evidence to be included in the Final Report of the AI.
Activate standard reporting vehicles	The plan should: • Name the Subject Matter Experts, or SMEs and Security Points of Contact (POCs) who should be contacted after an incident • Define the standard reporting vehicles for documentation of security violation
Implement clean-up plan	Cleanup should proceed as soon as possible to avoid further contamination, compromise, or loss once the data owner is notified of the incident. The contractor should follow the data owner's cleanup plan, or the DSS guidelines in the DAAPM if the data owner has not provided a cleanup plan. Hard drives involved in a classified spill must be wiped using a wiping utility capable of performing the DoD-approved three-time overwrite. The contractor may want to obtain a wiping utility in advance to be prepared.

AI for IS Security Violations

Steps of AI for IS Security Violations

As previously noted, the AI process for IS security violations is very similar to the general processes and guidelines for AIs, with some important differences. The following sections describe these specific differences.

Contractor Responsibilities

The following are contractor responsibilities during an AI for an IS security violation. Note that in addition to the company's FSO, the ISSM or Information

Technology network administrator, if there is no ISSM, should be involved in all AI activities when a security violation involves an IS.

- Contact the GCA/data owner for procedures and guidance
- Follow guidance in Paragraph 1-303 of NISPOM and the DAAPM
- Immediately call your ISSP/SCA and IS Rep
- Notify all involved facilities and personnel

Initial Report Requirements

In addition to the standard elements of the initial report, the contractor must include several elements specifically addressing the affected information system and information.

- Include description of security violation
- Describe all possibly affected IS/equipment and its current status
- Document events and corrective action and declassification
- Include data owner contact information
- Include approved cleanup procedures
- Submit report immediately, followed by final report within 15 days

Appendix B of the AI Process Guide provides a template for creating the report.

Term	Description
IS/equipment	For example: • Servers, workstations, notebooks, mobile devices, etc. • Remote dial-in or network connection • Back-up tapes involved • Availability of audit logs

Conducting the Administrative Inquiry (AI)

There are some special considerations when conducting an AI of a security violation involving an IS.

- ISSM interviews all users to discover:
  - The nature of the affected information
  - How the information was accessed and where it was stored
  - Whether the information was transferred to another media
  - The current location and status of the information and/or media
- Priorities are to identify:

    - What classified information was compromised and at what level
    - The GCA(s) for all associated contracts
- Additional AI activities include:
    - Making inventory of all affected memory and media and equipment
    - Communicating vulnerabilities to the IS Rep, ISSP/SCA, and CISA

Additional Response Activities

In addition to the AI activities, security violations involving IS require some very specific response activities in order to contain the data spill.

- Execute established protocols to have IT expert participate in interviews with involved individuals
    - Interview associated SMEs and INFOSYSSEC personnel
    - Document impact and extent of vulnerability of system
- Conduct sanitization and cleanup procedures as quickly as possible
    - Follow Cleanup Procedure Guidance provided by the GCA or data owner, or contained in the DAAPM if cleanup procedures were not provided
    - Station an appropriately cleared individual with the equipment that cannot be sanitized immediately (e.g., internal fixed disks).
    - DO NOT LEAVE ANY unsanitized equipment UNATTENDED

Term	Description
Cleanup Procedure Guidance	See DAAPM as appropriate: • Classified spills cleanup procedures • Contamination cleanup procedures • Specific cleaning checklists

Final Report Requirements

There are several different requirements for the Final Report of an AI for an IS security violation.

- Follow general guidance for Final Reports of AI
- The report should also include:
    - A summary of all actions taken
    - Current location of classified information
    - Description of networked systems and network configuration of impacted IS

- Any requirements made by data owner

See Administrative Inquiry (AI)/Security Violation Investigation Process Job Aid and DAAPM for more information.

Scenario

An FSO just learned about an IS security violation and is launching a preliminary inquiry. She has some questions about how to do it correctly and has come to you for some help.

Review Activity 1

The FSO says she knows her company has an incident response plan, but she's not sure how it will help her. What is the purpose of the incident response plan?

Select all that apply and then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Define reportable incidents
- ☐ Describe the security violation
- ☐ Describe the affected system and the associated network
- ☐ Define resources and management support required to respond
- ☐ Provide a roadmap for incident response capabilities

Review Activity 2

The FSO asks who is responsible for conducting the interviews during a typical inquiry of a violation involving an IS?

Select the best response and then check your answer in the Answer Key at the end of this Student Guide.

- ○ IS Rep
- ○ ISSM
- ○ FSO
- ○ ISSP/SCA

Review Activity 3

In addition to the inquiry of the violation, which other activities must occur following a security violation involving an IS?

Select all that apply and then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Notify all affected facilities and personnel
- ☐ Create a best practice report
- ☐ Contact GCA/data owner
- ☐ Notify ISSP/SCA

- ☐ Implement clean-up procedures
- ☐ Provide Training

Review Activity 4

Which entity provides guidance to contractors on authorized information systems and how to respond to security violations involving those systems?

Select the best response and then check your answer in the Answer Key at the end of this Student Guide.

- ○ Personnel Security Management Office (PSMO)
- ○ National Industrial Security Program Authorization Office (NAO)
- ○ Department of Defense Consolidated Adjudications Facility (DoD CAF)
- ○ National Security Agency (NSA)

Unauthorized Systems

Special Considerations

When handling security violations involving unauthorized systems, there are some special considerations that need to be taken into account. The contractor should consider having a second individual observe the procedures to assist with verification and ensure that no steps are missed. In certain special circumstances, such as for multi-user systems and when a classified file is discovered on an authorized system, there may be additional defined procedures to follow. Any wiping utility that will be used during cleanup must be able to perform a three-time overwrite. In all cases, the contractor should contact their ISSP/SCA to ensure corrective actions are adequate. Once the extent of the compromise has been determined and the exact locations of the information on the system are known, the contractor should begin sanitization procedures following the National Security Agency (NSA) guidelines for sanitization of each piece of equipment and media.

Multi-user System

For multi-user systems, depending on the suspected severity and magnitude of the problem:

- Stop all remote (dial-up) and local user processes OR
- Suspend processes until corrective actions are completed to protect users from losing work performed up to that time

Note: Some situations may not warrant stopping all local user processes. For example, having one classified number in email limited to a few terminals and the information was immediately deleted.

Classified Information Found

If a classified file is found on a system:

- Do NOT erase the file
- Identify the file name, creation/modification date, owner, and protection code
- Temporarily protect the file to the highest privilege level

DSS Involvement

DSS Roles and Responsibilities

When handling IS security violations, it is important that you are familiar with DSS involvement through the process. For all violations involving an IS processing classified information, the IS Rep will request the assistance of the ISSP/SCA in responding to the violation. The IS Rep and ISSP/SCA should respond to the facility within 72 hours when possible to support the contractor in conducting the AI. If the contractor's ISSM has a proven track record of handling cleanup in an expeditious and compliant manner, it may not be necessary that the assistance take place on-site at the contractor facility. The IS Rep and ISSP/SCA will also ensure that the facility uses appropriate cleanup procedures and will collaborate with the ISSM to determine the best overall containment solution.

Communicating with the GCA

In the event of a security violation involving an IS, it is essential that the IS Rep or contractor ISSM notify the GCA as soon as possible. This notification should take place immediately if any of the affected information is Top Secret; otherwise, it should occur within 72 hours. Communications and documentation describing the incident and confirmed or suspected classified data at risk are classified at the highest level of the data involved. The IS Rep should ensure use of secure communication channels if communications with the GCA would reveal file names, date or time groups on message headers, and whether the system is still contaminated. It is important to note that in incidents involving the inadvertent transmission of classified information to an uncleared company, DSS has no authority to act other than to notify the GCA. Under no circumstance will DSS notify the uncleared company they were sent classified information.

Conclusion

Lesson Summary

This concludes the lesson “Security Violations Involving Information Systems.”

Answer Key

Review Activity 1 (What is an IS Security Violation?)

Contractor Julie Williams has a CONFIDENTIAL clearance. While working on a specific assignment and conducting internet research using her work computer, she downloads a file that appears to be relevant to her assignment. As she reads through the document, she quickly realizes that the document contains SECRET information that should not be available to the public.

Which type of IS security violation does this scenario illustrate?

- ○ Unauthorized Access
- ○ Data Spills
- ○ Processing Classified Info on Unauthorized System
- ○ Suspicious Contacts
- ◉ Inadvertent Exposure (correct response)

Feedback: *This scenario is an example of inadvertent exposure. Julie did not intend to access classified information but inadvertently did so while conducting internet research.*

Review Activity 2 (What is an IS Security Violation?)

Employee Jeremy Wallace's computer has some issues and glitches that are being addressed by the company's Information Technology specialists. While his computer is unavailable, he's been using a nearby shared work station. A few hours later, it is brought to Jeremy's attention that the shared work station had not been authorized to process the types of classified information he had been working with.

Which type of IS security violation does this scenario illustrate?

- ○ Unauthorized Access
- ◉ Data Spills (correct response)
- ○ Suspicious Contacts
- ○ Inadvertent Exposure

Feedback: *This scenario demonstrates a data spill.*

Review Activity 1 (AI for IS Security Violations)

The FSO says she knows her company has an incident response plan, but she's not sure how it will help her. What is the purpose of the incident response plan?

- ☑ Define reportable incidents (correct response)
- ☐ Describe the security violation
- ☐ Describe the affected system and the associated network
- ☑ Define resources and management support required to respond (correct response)
- ☑ Provide a roadmap for incident response capabilities (correct response)

Feedback: *The purpose of the Incident Report is to define reportable incidents, define resources and management support required to respond, and provide a roadmap for incident response capabilities. Describing the violation and affected systems are done in the Initial and Final Reports of the security violation.*

Review Activity 2 (AI for IS Security Violations)

The FSO asks who is responsible for conducting the interviews during a typical inquiry of a violation involving an IS?

- ○ IS Rep
- ◉ ISSM (correct response)
- ○ FSO
- ○ ISSP/SCA

Feedback: *When a security violation involving IS occurs and the contractor has someone in this role, the ISSM is responsible for conducting interviews.*

Review Activity 3 (AI for IS Security Violations)

In addition to the inquiry of the violation, which other activities must occur following a security violation involving an IS?

- ☑ Notify all affected facilities and personnel (correct response)
- ☐ Create a best practice report
- ☑ Contact GCA/data owner (correct response)
- ☑ Notify ISSP/SCA (correct response)
- ☑ Implement clean-up procedures (correct response)
- ☐ Provide Training

Feedback: *Although creating a best practice report and providing training are good after action items, the remaining activities must be completed after an IS security violation involving an IS.*

Review Activity 4 (AI for IS Security Violations)

Which entity provides guidance to contractors on authorized information systems and how to respond to security violations involving those systems?

- ○ Personnel Security Management Office (PSMO)
- ◉ National Industrial Security Program Authorization Office (NAO)
- ○ Department of Defense Consolidated Adjudications Facility (DoD CAF)
- ○ National Security Agency (NSA)

Feedback: *The DSS National Industrial Security Program Authorization Office (NAO) provides guidance to contractors on authorized information systems and responding to security violations.*

Lesson 6

Course Summary

Summary

The National Industrial Security Program (NISP) relies on many individuals in both industry and government, in a wide range of roles, to share the responsibility of ensuring that all classified information remains secure. These government and contractor personnel work together to respond quickly and appropriately to security violations and conduct AIs as needed.

Lesson Review

Here is a list of the lessons in the course.

- Lesson 1: Course Introduction
- Lesson 2: Security Violations Overview
- Lesson 3: Initial Reporting of Security Violations
- Lesson 4: Administrative Inquiry Process
- Lesson 5: Security Violations Involving Information Systems
- Lesson 6: Course Conclusion

Course Conclusion

Congratulations. You have completed the *NISP Security Violations and Administrative Inquiries* course.

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

- Define security violation and identify types of violations
- Identify roles and responsibilities in conducting administrative inquiries
- Identify the steps in security violation report processing and conducting administrative inquiries
- Conduct administrative inquiries of security violations
- Identify special considerations in conducting administrative inquiries of security violations involving authorized information systems

To receive credit for this course, you *must* take the *NISP Security Violations and Administrative Inquiries* examination. Follow the instructions on screen to access the online exam.