Student Guide

# NISP Security Violations and Administrative Inquiries

## *Lesson 1: Course Introduction*

### Contents

# 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 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 administrative inquiry refers specifically to the DSS inquiry process; however, this term 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 (ISSPs)
- DSS Counterintelligence (CI) Personnel
- Other DoD Security Specialists with Industrial Security responsibilities

Although these roles are distinct and have diverse responsibilities, they require a shared baseline understanding of security vulnerability assessments 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

Student Guide

# NISP Security Violations and Administrative Inquiries

## *Lesson 2: Security Violations Overview*

### Contents

# 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, of the Administrative Inquiry, 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 whether the classified information was at risk of compromise, the individual or individuals responsible for the violation, and whether 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 a security violation investigation or action.

## 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.<br>*NOTE: Classified information sent via unencrypted email is considered lost.*<br>*Examples:*<br>A courier stopped at a restaurant for lunch and forgot to lock the car; as a result, a classified package was stolen and has not been returned or located.<br>An engineer went to the safe 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).<br>*Example:*<br>A SECRET document left on the copier machine is found by an uncleared employee. |
| **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.<br>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.<br>*Example:*<br>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 (ISSP)
- Counterintelligence Special Agent (CISA)
- Government Contracting Activity (GCA)
- Personnel Security Management Office for Industry (PSMO-I)
- DoD Consolidated Adjudication Facility (DoD CAF)

### FSO

When a security violation occurs, the FSO is responsible for conducting a preliminary inquiry. 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 security assessment. If loss, compromise, or suspected compromise did occur, the FSO must notify the DSS field office of the violation and submit the initial and final reports. If a culpable employee is identified, the FSO must also submit a culpability report.

| Term | Definition |
|---|---|
| **Culpable Employee** | In accordance with NISPOM 1-304, an individual may be found culpable for a security violation if there is evidence of one or more of the following factors:<br>• Deliberate disregard of security requirements<br>• Gross negligence in the handlings of classified material<br>• A pattern of negligence or carelessness |

**ISSM**

During the course of a security violation investigation, if the violation involved an accredited information system, the ISSM must:

- 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 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**

When requested, the ISSP assists the IS Rep with violations involving information systems processing classified information. The ISSP'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 accredited 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 submits classification review and damage assessment results to DSS.

### PSMO-I

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

- Processes security violation in which individual culpability is determined
- Places information into Case Adjudication Tracking System (CATS) and forwards in Joint Personnel Adjudication System (JPAS) to DoD CAF as appropriate for adjudication

### DoD CAF

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

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

# 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 unapproved and unaccredited 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

# 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 unapproved and unaccredited 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 unsecured network, 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

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

Student Guide

# NISP Security Violations and Administrative Inquiries

## *Lesson 3: Initial Reporting of Security Violations*

### Contents

# 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 roles and responsibilities in conducting administrative inquiries/security violation investigations
- 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 security vulnerability assessment.

### *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 involved classified information, including contract number, procurement activity, and 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)
- Notifies involved or affected DSS Regional Director and Field Offices
- Provides a copy of the preliminary report to:
  - Field Office Chief (FOC)
  - Local CI Special Agent (CISA)
  - Local ISSP, 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 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 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

## 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

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

Student Guide

# NISP Security Violations and Administrative Inquiries

## *Lesson 4: Administrative Inquiry Process*

### Contents

# Introduction

### *Lesson Objectives*

In this lesson, you will walk through the steps of conducting an inquiry of a security violation.

Here are the lesson objectives.

- Conduct administrative inquiries 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 Processing Requirements
  - 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 (ISSP), 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 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, then 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 administrative inquiry 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, prevent future violations, and discipline culpable individuals.

### *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 for Industry (PSMO-I) via the Joint Personnel Adjudication System (JPAS).

To view additional information on how this is done, please refer to CDSE's webinar on How to Submit an Incident Report Within JPAS and the DSS PSMO-I page on Incident Reports, both 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 sections 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<br>• When and where the inquiry was conducted<br>• Who conducted the inquiry |
| **Essential Facts** | • A description of the circumstances surrounding the violation and NISPOM provisions that were violated<br>• Who was involved, including level and type of personnel clearance of the individuals involved<br>• When and where the violation occurred<br>• All affected classified information |

| Section | Description |
|---|---|
| **Corrective Actions** | • Summary of the corrective actions taken by the facility<br>• Specific actions initiated or taken by the facility to secure the information after the violation was discovered<br>• Any disciplinary actions taken against the culpable individual(s) involved in the security violation and description of the graduated scale of disciplinary actions<br>• Notification of and coordination with the GCA |
| **Conclusions** | • Formal determination for each security violation as previously identified (loss, compromise, suspected compromise, no compromise)<br>• Vulnerability of classified information<br>• Description of unauthorized access<br>• Description of GCA Classification Review |
| **Determination of Culpability** | • Procedures followed to investigate the individual(s) involved in the security violation<br>• Whether the violation involved:<br>o Deliberate disregard for security requirements<br>o Gross negligence<br>o Pattern of negligence<br>• The individual(s) involved in the violation<br>o Description of individual actions<br>o Awareness of NISPOM and associated security guidelines, policies, and provisions<br>o Notification of PSMO-I |
| **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, CISA, Field Office Chief, and Regional Director. If culpability is

identified, then the IS Rep will provide PSMO-I with a copy of the final report within five days of closure of the violation.

**PSMO-I**

The final report is submitted to PSMO-I 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 Administrative Inquiry 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-I 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-I 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-I 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.*

Student Guide

# NISP Security Violations and Administrative Inquiries

## *Lesson 5: Security Violations Involving Information Systems*

### Contents

# Introduction

### *Objectives*

In a world driven by technology, it can be expected that there will be incidents of security violations involving information systems. It is important to know what considerations need to be made when addressing security violations involving accredited information systems.

Here are the objectives for this lesson.

- Recognize types of IS Security Violations
- Identify components of an Incident Response Plan
- Identify additional requirements and activities for violations involving information systems
- Identify special consideration for security violations involving nonaccredited systems
- Recognize when ISSP 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 information systems. 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 accredited and non-accredited information systems 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 Office of the Designated Approving Authority (ODAA) 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 ODAA Process Manual.

## *Types of IS Security Violations*

Let's first take a look at the different types of information system 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 accredited 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 loses its accreditation and the processing of classified information continues
- The FSO and ISSM/ISSP are responsible 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.

**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 with which he had been working.

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 Plans

### *Purpose*

To mitigate violations should they occur, contractors with accredited information systems should have an incident response plan in place.

The purpose of an Incident Response Plan is to

- Provide a roadmap for implementing response capability
- Describe the structure of response capability
- Provide a high-level approach for how the incident response 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 Incident Response Plan and the specific response procedures. To quickly respond to security violations should they occur, the Incident Response Plan should contain points of contact, notification requirements, and cleanup procedures. The contractor should coordinate with the 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, and disseminating the plan to appropriate personnel. The guidelines for cleanup should be implemented as soon as possible to avoid further contamination.

Copies of the Incident Response 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 Administrative Inquiry Guidelines for Information Systems and ODAA Process Manual, 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). |
| **Create event logs and back-up databases** | The plan should address the:<br>• Location and retrieval methods for IS Event Log(s) and back-up databases for evaluation<br>• Restoration of records, files, and/or applications<br>The Event Log can provide additional evidence to be included in the Final Report of the administrative inquiry. |
| **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. |
| **Activate standard reporting vehicles** | The plan should:<br>• Name the SMEs and Security POCs who should be contacted after an incident<br>• Define the standard reporting vehicles for documentation of the security violation |
| **Implement clean-up plan** | Clean-up 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 ODAA Process Manual 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 administrative inquiries, 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 information systems.

- Contact the GCA/data owner for procedures and guidance
- Follow guidance in Paragraph 1-303 of NISPOM and ODAA Process Manual
- Immediately call DSS ISSP and inform your DSS 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
- Be submitted 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:<br>• Servers, workstations, notebooks, mobile devices, etc.<br>• Remote dial-in or network connection<br>• Back-up tapes involved<br>• Availability of audit logs |

### Conducting the Administrative Inquiry

There are some special considerations when conducting an AI of a security violation involving 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, 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 INFOSEC 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 ODAA Process Manual 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 ODAA Process Manual Section 4.5, as appropriate:<br>• Classified spills cleanup procedures<br>• Contamination cleanup procedures<br>• Specific cleaning checklists available in Sections 14.1.17-21 |

### 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) Process Job Aid and ODAA Process Manual 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

### *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
- ☐ Contact GCA/data owner
- ☐ Notify ISSP
- ☐ Implement clean-up procedures

### *Review Activity 4*

Which entity provides guidance to contractors on accredited 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.*

- ○ PSMO-I
- ○ ODAA
- ○ DoD CAF
- ○ NSA

# Non-accredited Systems

## *Special Considerations*

When handling security violations involving non-accredited 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 unaccredited 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 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 information systems processing classified information, the IS Rep will request the assistance of the ISSP in responding to the violation. The IS Rep and ISSP should respond to the facility within 72 hours when possible to support the contractor in conducting the administrative inquiry. 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 will also ensure that the facility uses appropriate cleanup procedures and will collaborate with the ISSM to determine the best overall containment solution.

## *Notifying the GCA*

In the event of a security violation involving 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 with which he had been working.

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

***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)
- ☑ Contact GCA/data owner (correct response)
- ☑ Notify ISSP (correct response)
- ☑ Implement clean-up procedures (correct response)

***Feedback:*** *All of these activities must be completed after a security violation involving an IS.*

### *Review Activity 4 (AI for IS Security Violations)*

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

- ○ PSMO-I
- ◉ ODAA (correct response)
- ○ DoD CAF
- ○ NSA

***Feedback:*** *The DSS Office of the Designated Approving Authority (ODAA) provides guidance on contractor accredited information systems and responding to security violations.*

Student Guide

# NISP Security Violations and Administrative Inquiries

## *Lesson 6: Course Conclusion*

### Contents

# Course Summary

## *Summary*

The National Industrial Security Program 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 administrative inquiries 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

## *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 accredited information systems

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

Glossary

# NISP Security Violations and Administrative Inquiries

**Access**: The ability and opportunity to gain knowledge of classified information

**Adjudication**: Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted or retain eligibility for access to classified information, and continue to hold positions requiring a trustworthiness decision

**Administrative Inquiry**: Formal investigation of a possible loss, compromise or suspected compromise

**Adversary**: An individual, group, organization, or government that must be denied Critical Program Information (CPI). Synonymous with competitor/enemy.

**Authority**: The reason for an inquiry, when and where it was conducted, and who conducted the inquiry

**Carelessness**: Failure to give sufficient attention to avoiding harm or errors; negligence

**Classified Information**: Official information that has been determined, pursuant to Executive Order 12958 or any predecessor order, or pursuant to the Atomic Energy Act of 1954, to require protection against unauthorized disclosure in the interest of national security which has been designated

**Classification Review**: Review of compromised classified information to determine whether affected information should be declassified or downgraded and identify measures to protect against threat to national security

**Clearance**: An administrative authorization for access to National Security Information (NSI) up to a stated classification level (TOP SECRET, SECRET, CONFIDENTIAL)

**Cleared Employees**: All contractor employees granted PCLs and all employees being processed for PCLs

**Cognizant Security Agencies (CSAs)**: Agencies of the Executive Branch that have been authorized by Executive Order 12829 to establish an industrial security

program to safeguard classified information under the jurisdiction of these agencies when disclosed or released to U.S. Industry. These agencies are The Department of Defense, Office of the Director of National Intelligence, Department of Energy, Nuclear Regulatory Commission, and Department of Homeland Security.

**Cognizant Security Office (CSO)**: The organizational entity delegated by the head of a CSA to administer industrial security on behalf of the CSA

**Compromise**: An unauthorized disclosure of information. A compromise is a confirmed disclosure of specifically identifiable classified information to specified unauthorized individuals(s).

**Conclusion**: A formal determination for each security violation as previously identified (loss, compromise, suspected compromise). Define the security violation as a Loss, Compromise, Suspected Compromise, or No Loss, Compromise, or Suspected Compromise. Include vulnerability of information, description of unauthorized access, and description of GCA classification review.

**CONFIDENTIAL**: The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to National Security that the Original Classification Authority (OCA) is able to identify or describe

**Containment**: Keeping security violations from harming other programs or individuals

**Contractor**: Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA

**Corrective Actions**: Any disciplinary actions taken against a culpable individual(s) involved in a security violation and the actions initiated or taken by the facility to secure the information after the violation

**Culpable Person**: An individual involved in a security violation that has been determined to have displayed a deliberate disregard for security requirements, had a pattern of negligence, or was grossly negligent in their duties

**Damage Assessment**: The analysis of the impact on national security because of the disclosure of classified information to an unauthorized person

**Data Spill**: Known also as contaminations or classified message incidents, occurs when classified data or controlled unclassified data (CUI) is introduced to an unclassified computer system or to a computer system accredited at a lower classification level than the data being entered

**Declassification**: The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation

**Defense Security Service (DSS)**: An agency of the Department of Defense (DoD) located in Quantico, Virginia with field offices throughout the United States. The Under Secretary of Defense for Intelligence provides authority, direction, and control over DSS. DSS provides the military services, defense agencies, 30 federal agencies and approximately 13,500 cleared contractor facilities with security support services. DSS is the CSO for most DoD classified contracts.

DSS supports the National Security and the warfighter, secures the nation's technological base, and oversees the protection of U. S. and foreign classified information in the hands of industry. DSS accomplishes this mission by clearing industrial facilities, accrediting information systems, facilitating the personnel security clearance process, delivering security education and training, and providing information technology services that support the industrial and personnel security missions of DoD and its partner agencies.

**Defense Security Service, Center for Development of Security Excellence (CDSE)**: Responsible for providing security education and training to DoD and other U.S. government personnel, DoD contractors, and sponsored representatives of foreign governments

**Defense Security Service, Counterintelligence (CI) Office**: Office within the Defense Security Service that provides counterintelligence support to DSS through CI reviews, assessments, analysis, and reports

**Defense Security Service, Field Counterintelligence Specialist (FCIS)**: Assists FSOs in identifying potential threats to U.S. technology and developing CI awareness and reporting by company employees

**Defense Security Service, Field Office Chief (FOC)**: Manages the field offices that are staffed by Industrial Security Representatives (IS Reps). The Field Office Chief is responsible for ensuring that each facility is assigned an IS Rep.

**Defense Security Service, Industrial Security Representative (IS Rep)**: Local representative from the Defense Security Service that provides advice and assistance on security matters and with establishing your security program to ensure your facility is in compliance with the NISP

**Defense Security Service, Information Systems Security Professional (ISSP)**: Local representative from the Defense Security Service, Office of Designated Approving Authority (ODAA) that provides advice and assistance visits to improve the security posture with regard to Information Systems and help facilitate the

process of getting your information systems accredited to process classified information

**Defense Security Service, Office of Designated Approving Authority (ODAA)**: Office within the Defense Security Service that facilitates the certification and accreditations process for information systems at cleared contractor facilities

**Defense Security Service, Personnel Security Management Office for Industry (PSMO-I)**: Office within the Defense Security Service that processes requests for and other actions related to personnel security clearances for personnel from facilities participating in the NISP

**Defense Security Service, Regional Director**: A DSS employee that has overarching responsibility of one of the four DSS geographical regions: Capital, Northern, Southern, and Western

**Department of Defense**: The largest Cognizant Security Agency (CSA) with the most classified contracts with industry

**Department of Defense Consolidated Adjudication Facility**: Responsible for issuing a clearance authorization for eligible individuals

**DoD Security Specialist**: Also called Activity Security Managers. Act as the GCA representatives to the NISP and serve as resident security subject matter experts (SMEs).They also maintain security cognizance over all activity information, personnel, information systems, physical security and industrial security.

**Downgrading**: A determination by a Declassification Authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level

**Eligibility**: A DoD Consolidated Adjudication Facility (DoD CAF) has made an adjudicative determination of member's Personnel Security Investigation (PSI) and that member may have access to classified information equal to the level of their adjudicated investigation.

**Essential Facts**: Provide description of the circumstances surrounding the violation, the relevant sections of the NISPOM that were violated, who was involved, and when and where the violation occurred. Include the level and type of personnel clearance of the individuals involved in the occurrence.

**Espionage**: The act or practice of spying or of using spies to obtain secret intelligence. Overt, covert, or clandestine activity, usually used in conjunction with the country against which such an activity takes place (e.g., espionage against the United States (U.S.)).

**Executive Order (EO)**: An order issued by the President to create a policy and regulate its administration within the Executive Branch

**Facility**: A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For the purposes of industrial security, the term does not include Government installations.

**Facility Security Officer (FSO)**: A U.S. citizen employee, appointed by a contractor who will supervise and direct security measures necessary for implementing the NISPOM and other Federal requirements for classified information

**Federal Bureau of Investigations (FBI)**: An intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities—the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community

**Foreign Involvement**: The fact or condition of being involved with a foreign country

**Freedom of Information Act (FOIA)**: A provision that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records, or portions thereof, are protected from disclosure by one of nine exemptions

**Government Contracting Activity (GCA)**: An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions

**Inadvertent Exposure**: A set of circumstances or a security incident in which a person has had involuntary access to classified information that he or she was or is not normally authorized

**Industrial Security**: That portion of information security concerned with the protection of classified information in the custody of U.S. industry

**Industrial Security Facility Database (ISFD)**: System of record for facility clearance information

**Information Security**: The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by Executive Order

**Information System**: An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material

**Information System Security Manager (ISSM)**: An individual appointed by a contractor with oversight responsibility for the development, implementation, and evaluation of the facility's information system security program. The ISSM must be trained to a level commensurate with the complexity of the facility's information systems.

**Investigation**: The action of investigating something or someone; formal or systematic examination or research

**Joint Personnel Adjudication System (JPAS)**: The DoD system of record for contractor eligibility and access for personnel security clearances

**Key Management Personnel (KMP)**: Senior management identified in a facility that require an eligibility determination in order for a facility to be granted a facility clearance. Facility Security Officers (FSOs) are considered KMP.

**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

**National Industrial Security Program (NISP)**: Established by Executive Order 12829 for the protection of classified information released or disclosed to industry in connection with classified contracts. The NISP applies standards for the protection of classified information released or disclosed to contractors of all federal executive branch departments and agencies. Requirements of the NISP are stated in the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M.

**National Industrial Security Program Operating Manual (NISPOM)**: A manual issued in accordance with the National Industrial Security Program that prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified of classified information

**National Security Agency (NSA)**: Provides information assurance services and information and signals intelligence

**Negligence**: Failure to use reasonable care, resulting in damage, loss or injury to another

**Original Classification Authority (OCA)**: An individual authorized in writing, either by the United States (U.S.) President, or by agency heads or other officials designated by the President, to classify information in the first instance. OCAs must receive training to perform this duty.

**Preliminary Inquiry**: Done to secure the classified information and gather all the facts to determine if there was a loss, compromise, or suspected compromise

**Sabotage**: The willful destruction of government property with the intent to cause injury, destruction, defective production of national defense, or war materials by either an act of commission or omission

**Safeguarding**: Controls that are prescribed to protect classified information

**SECRET**: The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to National Security that the Original Classification Authority (OCA) is able to identify or describe

**Security Violation**: A failure to comply with the policy and procedures established by the NISPOM that reasonably could result in the loss or compromise of classified information

**Security Vulnerability Assessment**: Reviews of contractor security programs to ensure security counter measures are in place to mitigate hostile intelligence threats and ensure national policy compliance

**Security Training Education and Professionalization Portal (STEPP)**: The learning management system used by the Center for Development of Security Excellence (CDSE). STEPP is where the list of courses is maintained and where student information and course transcripts are maintained.

**Special Access Program (SAP)**: Any program that is established to control access and distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A SAP can be created or continued only as authorized by a senior agency official delegated such authority pursuant to the NISPOM.

**Subject Matter Expert (SME)**: An expert in a particular field who contributes or verifies the accuracy of specific information needed by the project team

**Subversion**: An attempt to transform the established social order and its structures of power, authority, and hierarchy

**Suspected Compromise**: Occurs whenever identifiable classified information has been made available to unauthorized individual(s) who may have gained access to the information

**Suspicious Contact**: Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country

**Technology**: The information and know-how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or manuals, or in intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data, but not the goods themselves, or the technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and computer software

**Terrorism**: The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological

**Threat**: Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or Denial of Service (DOS)

**TOP SECRET**: The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to National Security that the Original Classification Authority (OCA) is able to identify or describe

**Unauthorized Access**: A communication or physical transfer of classified information to an unauthorized recipient