Security Incidents in the NISP Short

Student Guide

October 2024

Center for Development of Security Excellence

Contents

Introduction

[Jacob] Excuse me? Are you the FSO? I'm Jacob, Sherri's new administrative assistant. I just came in, and I saw this document on the table outside her office. It reads SECRET on the cover. In our security training we were told to report this type of incident to the Security Office. I guess that means you.

[Narrator] Under the National Industrial Security Program, or NISP, contractors with access to classified information have the responsibility to safeguard that information. When a security incident occurs that threatens to compromise that information, you have the responsibility to protect the information, report the incident, investigate the circumstances of the incident, and work with the Defense Counterintelligence and Security Agency, or DCSA, to mitigate the damage.

In this Short, you take on the role of a Facility Security Officer, or FSO, to learn this process. Along the way you will meet many of the other roles that will assist you. When you have completed the Short, you should be able to follow the required procedures to report and investigate security incidents.

Learning Objective: Given a scenario, follow the process for reporting and investigating security incidents.

Incident Preparation

It's crucial for cleared contractors to have an Incident Response Plan, or IRP, in place as part of your company's Standard Practice Procedure, or SPP. Per the National Industrial Security Program Operating Manual, or NISPOM, your SPP must include specific reporting requirements. You must report any loss, compromise, or suspected compromise of classified information, whether domestic or foreign, to your Cognizant Security Agency, or CSA. The IRP also identifies an Incident Response Team who will be properly trained to respond to security incidents.

Who Responds to Incidents?

Let's look at some of the people inside and outside your organization who will respond to security incidents.

Incident Response Team

As the FSO for your company, you will take a lead role in any security incident response. You will be supported by your Insider Threat Program Senior Official, or ITPSO, your Information System Security Manager, or ISSM (if your organization has authorized classified information systems), and the Senior Management Official, or SMO. Your Incident Response Team may also include Program Managers; other Subject Matter Experts, or SMEs; and other Information Technology, or IT personnel.

Department of Defense

You won't be responding to incidents alone. The DCSA personnel within your CSA will work with you to ensure classified information is secure and the process is followed correctly. This includes your Industrial Security Representative, or IS Rep; Information System Security Professional, or ISSP; and Counterintelligence Special Agent, or CISA. Personnel from your Government Contracting Activity, or GCA, will also work with you through this process. This may include DOD Component Security; counterintelligence, or CI, points of contact, and your Original Classification Authority, or OCA.

Immediate Responsibilities

Now think back to the situation. An administrative assistant has brought you a SECRET document that was left unsecured. As the FSO, what do you do?

Your first and most important responsibility is to secure the material. You must isolate all involved material and safeguard it from further loss. In our scenario, this is a physical document, so you will place it in a secure location per the NISPOM, which should also be described in your IRP.

You and your Incident Response Team have several other responsibilities immediately after the incident. These include:

- Initiating incident response procedures,
- Confirming the information is classified,
- Determining if the classified information is in the public domain,
- Noting the details about the incident,
- Identifying anyone else involved,
- Notifying the involved parties,
- Notifying individuals not to access the information, and
- Confirming the applicable CSA.

Initiate IRP Procedures

Your IRP should include specific procedures for physical or digital information loss. DCSA can provide minimum acceptable procedures, but procedures in your organization's IRP should be detailed and specific to the cases you may face.

Confirm Classification

Confirm that the information is in fact classified and the level of classification. This is an important step to gauge the extent of the potential damage of any loss or compromise. If information systems are involved in the incident, it is especially important not to wait to take action. Information can travel quickly.

In this scenario, the classified document that Jacob found and brought to you contains specifications for equipment your organization generates for a DOD classified contract. This information is classified at the SECRET level per the DOD Contract Security Classification Specification, DD Form 254.

Check Public Domain

Determine whether the classified information has reached the public domain.

There is no indication that the information Jacob found has reached the public domain. If you do find it has reached the public domain, you can find further guidance from DCSA's Notice to Cleared

Contractors Under the National Industrial Security Program on Inadvertent Exposure to Potentially Classified Information in the Public Domain.

Refer to the Short Resources page to access the Notice.

Collect Incident Details

Note where the material was found, when, and by whom.

Jacob found the document outside your Chief Executive Officer, or CEO, Sherri's office at 7:58 am on Friday and brought it to you immediately.

Identify Others Involved

Identify any people, devices, systems, and cleared contractors involved in the incident.

For the document Jacob found, no devices or systems seem to be involved, but you will need to identify exactly who left the information and who might have encountered it.

Notify Involved Parties

Notify all parties involved that there has been an incident with the material.

Instruct Not to Access

Instruct individuals not to attempt to access the information.

For the document Jacob found, you will send this instruction to anyone using this information for their work projects.

Confirm CSA

Confirm your CSA. DCSA is the CSA for contractors. The CSA may also be determined by reviewing the DD Form 254.

In this case, you will work with DCSA.

Knowledge Check 1

After Jacob informs you of the unsecured SECRET document, what action should you take first?

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

○ Notify all involved parties
○ Isolate and safeguard the material
○ Create a team of individuals properly trained to deal with incidents
○ Identify any devices or systems involved

Knowledge Check 2

Who should be part of your Incident Response Team?

Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

- □ Facility Security Officer (FSO)
- □ Insider Threat Program Senior Official (ITPSO)
- □ Senior Management Officials (SMOs)
- □ Program Managers

Types of Security Incidents

As you look more deeply into the security incident, you will reach one of several possible outcomes:

- loss,
- compromise,
- suspected compromise,
- or no compromise.

A loss of information occurs when classified information cannot be accounted for or physically located. For a physical document, this would mean the document's location is unknown. For digital information, such as a computer file or email, a loss can occur when the information is transmitted through unsecure means.

The information becomes compromised when there has been a confirmed unauthorized disclosure of the information. A classified paper document shown to an uncleared person, or a digital file downloaded and opened on a system not authorized to process classified files are examples of compromised information.

A suspected compromise means the circumstances indicate the information could have been compromised, but it has not yet been confirmed. It can be difficult to prove that unauthorized access took place, so consider whether the facts of the case would lead a reasonable person to conclude that unauthorized access more than likely occurred.

If you can confirm through the facts that there was no risk of loss or compromise of classified information, then you can come to a conclusion that No Compromise occurred.

Infractions vs. Violations

The severity of an incident depends on whether the loss or compromise of classified information occurred or was likely.

If you confirm there has been no loss or compromise of the information, and there reasonably could not have been a compromise, the security incident may be called a Security Infraction. Even an infraction must still be reported and investigated to correct potential weaknesses in your company's security program. It may also reveal a recurring pattern of questionable judgement, irresponsibility, negligence, or carelessness by persons who have failed to comply with security policies and procedures.

If the security incident resulted in the loss or compromise of information, or there was a reasonable risk of loss or compromise this would be a Security Violation.

Initial Investigation

As the FSO, once you've secured the material and completed all initial steps and procedures, your responsibility will be to conduct a preliminary inquiry and submit an Initial Report to DCSA.

Your first priority in a preliminary inquiry is to gather all relevant facts about the incident, including the people, places, systems, and chain of events involved. You started this process already in your immediate responsibilities. Using these facts, you will determine whether there was a loss, compromise or suspected compromise of classified information. You will also classify the security incident as an infraction or a violation.

With the inquiry completed, you will complete an Initial Report and submit it to DCSA. The Initial Report will identify the nature of the security incident and when the incident occurred. It will provide a listing of all classified information involved in the incident, along with the GCA that has cognizance over the information and their contact information.

Conducting Interviews

As part of your initial inquiry, you will need to interview the people involved to understand the circumstances of the incident. This includes interviewing the Project Manager who misplaced the information, the Administrative Assistant who found it, and the CEO whose office is near where the information was found.

Jeff – Project Manager

[Jeff] I can't believe this. I've never done anything like this. I must have left the document on the table by Sherri's office Thursday afternoon.

I was in the conference room for a project meeting from two to three that afternoon. When the meeting was over, Samantha from the software team caught me in the hallway and asked me a question, and I guess I got distracted and put the document down on the table, and then I had to rush to arrive on time at another meeting offsite.

I always lock classified documents in the security container that's in my office.

Jacob – Admin. Assistant

[Jacob] I wasn't in on Thursday, so I don't know when the document was left there. I came in Friday morning just before eight, and I saw the document right away. It read SECRET on the top and bottom of the cover.

Our FSO told us in training, any classified information we find left unsecured must be reported to the Security Office, so that's where I went with it.

Sherri – CEO

[Sherri] I spent Thursday afternoon at our Springfield site, so I never saw the document. Jacob told me immediately when I got in the office on Friday.

You say Jeff left it there? That's disappointing. He's doing a great job leading this project, but he's failed to follow procedures before. Nothing this serious. This is his first time on a SECRET level project, so I know he's had security training on this recently.

Next Steps

The first step after your initial investigation is to submit your Initial Report to DCSA.

Your next step will be determined by the findings of your inquiry, depending on the type of incident. If the facts of your inquiry indicate the incident is a security infraction— and there is no loss or compromise of the information—prepare and submit a Final Report to DCSA with all of the relevant facts. We will cover the contents of the Final Report later in this Short. If the facts of your inquiry indicate a security violation likely took place—or you cannot rule out a loss or compromise of the information—conduct an in-depth investigation to uncover all possible facts in the incident. At the conclusion of your investigation, you will prepare and submit a Final Report documenting your findings.

If your initial investigation cannot gather sufficient information to come to a conclusion, prepare an Initial Report with whatever information you can and submit it within the mandatory deadline for the information involved. For an incident involving TOP SECRET information, you must submit an Initial Report within 24 hours or 1 calendar day. For SECRET or CONFIDENTIAL information, the Report must be submitted within 72 hours, or 3 calendar days. Then continue your investigation.

Knowledge Check 3

Recall that Jacob found an unsecured SECRET document on a table outside the CEO's office. The preliminary inquiry could not immediately rule out suspected compromise. Is this security incident an infraction or a violation?

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

○ Infraction

○ Violation

Knowledge Check 4

Because this is a security violation, what additional steps will you need to take?

Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

□ Sanction Jacob for accessing information without authorization

□ Conduct an investigation

□ Prepare and submit a Final Report

□ Submit the Initial Report

Corrective Actions

After submitting your Initial Report, you will conduct an in-depth investigation. If your investigation confirms there has been a security violation, disciplinary action will need to be taken against any culpable individuals to prevent a recurrence. These measures must comply with the graduated disciplinary policies established by your organization’s SPP and the NISPOM.

If employees meet the criteria in the NISPOM, you must submit an Individual Culpability Report to DCSA via the DOD Personnel Security System of Record. This includes whether the violation involved a deliberate disregard of security requirements, negligence in the handling of classified material, or a recent or recurring pattern of questionable judgment, irresponsibility, negligence, or carelessness.

Remedial security training may also be appropriate for the culpable employee to ensure they understand the importance of following security procedures and safeguarding classified information.

Submitting the Final Report

You will submit your Final Report to your DCSA IS Rep no later than 30 calendar days after the Initial Report. If an extension is necessary, you may request one by providing written justification to your IS Rep and/or ISSP.

The Final Report must include:

- References to DCSA-approved procedures;
- A summary of who, what, when, where, why, and how the violation occurred;
- A sequence of events tracing the violation from start to finish, documenting
  - Specific provisions violated,
  - Personnel and locations involved,
  - How unauthorized access was achieved,
  - If applicable, all IT-specific information, and
  - All involved classified information.
- Your conclusions from your investigation, including
  - Your determination of loss, compromise, suspected compromise, or no loss or compromise;
  - A description of the unauthorized access, if any;
  - The extent of the compromise; and
  - The date or time period the information was lost or at risk. The report should also include
  - Your determination of responsibility or culpability, including whether the individuals were involved in previous violations;

- Corrective and disciplinary actions taken or planned to prevent recurrence; and
- Supporting information that may be relevant to DCSA's final assessment, including details about information systems involved.

DCSA will summarize the violation and provide a Final Report to the GCA.

Knowledge Check 5

When must the Final Report be submitted to DCSA?

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

○ Within 24 hours of submitting the Initial Report.

○ Within 72 hours of submitting the Initial Report.

○ Within 14 days of submitting the Initial Report.

○ Within 30 days of submitting the Initial Report.

Conclusion

Congratulations. You have completed the Security Incidents in the NISP Short.

In this Short, you learned about the different roles and responsibilities involved in responding to security incidents. Remember, everyone who could come into contact with classified information needs to be aware of their responsibilities in the event of a security incident. A quick, competent response is essential to safeguard our nation's classified information.

You should now be able to follow the process for reporting and investigating security incidents.

Appendix A: Answer Key

Knowledge Check 1

After Jacob informs you of the unsecured SECRET document, what action should you take first?

○ Notify all involved parties
⦿ Isolate and safeguard the material (correct response)
○ Create a team of individuals properly trained to deal with incidents
○ Identify any devices or systems involved

Feedback*: Your first responsibility is to isolate and safeguard the classified material against any further loss or compromise.*

Knowledge Check 2

Who should be part of your Incident Response Team?

☑ Facility Security Officer (FSO) (correct response)
☑ Insider Threat Program Senior Official (ITPSO) (correct response)
☑ Senior Management Officials (SMOs) (correct response)
☑ Program Managers (correct response)

Feedback*: All of these people should be part of your Incident Response Team.*

Knowledge Check 3

Recall that Jacob found an unsecured SECRET document on a table outside the CEO's office. The preliminary inquiry could not immediately rule out suspected compromise. Is this security incident an infraction or a violation?

○ Infraction
⦿ Violation (correct response)

Feedback*: This is a violation because a classified document left unattended in an unsecured location could easily have been compromised. This will require further investigation.*

Knowledge Check 4

Because this is a security violation, what additional steps will you need to take?

□ Sanction Jacob for accessing information without authorization
☑ Conduct an investigation (correct response)
☑ Prepare and submit a Final Report (correct response)
☑ Submit the Initial Report (correct response)

Feedback*: You will submit the Initial Report, conduct your investigation, and then submit your Final Report at the conclusion of the investigation.*

Knowledge Check 5

When must the Final Report be submitted to DCSA?

○ Within 24 hours of submitting the Initial Report.

○ Within 72 hours of submitting the Initial Report.

○ Within 14 days of submitting the Initial Report.

⦿ Within 30 days of submitting the Initial Report. (correct response)

Feedback*: You have up to 30 days after submitting the Initial Report to submit the Final Report. You may request an extension if necessary by providing a written justification to your Industrial Security Representative and/or Information Systems Security Professional.*