Student Guide

Short: Special Access Program (SAP) Security Incidents

Objectives	• Given information about a possible security incident determine the type of incident • Given a specific security incident select appropriate next steps
Estimated completion time	10 minutes

Introduction

You are a government employee working in a Special Access Program Facility (SAPF), which encompasses the entire second floor of your building. Your work requires you to have a Secret clearance and access to SECRET//SAR-Red Train material. Visitors to the building are greeted at the receptionist's desk on the first floor; this area is unclassified.

The Government SAP Security Officer (GSSO) is conducting refresher security briefings this week and has placed copies of DoDM 5205.07 V1 in all employees' cubicles. Select the DoDM 5205.07 V1 at any time to review SAP security incident definitions and reporting requirements.

Welcome to the security brief.

I want to remind you of the importance of being able to recognize a SAP security incident and to take appropriate action. As you know, only the second floor of this building is a designated SAPF.

There are security violations and security infractions. They are both serious, and we want to minimize them as much as possible. Formal definitions of the two types of security incidents can be found in DoDM 5200.01, V3.

Essentially, an infraction is a security incident involving failure to comply with requirements (which cannot reasonably be expected to) and does not, result in the loss, suspected compromise, or compromise of classified information. An Infraction may be unintentional or inadvertent. If left uncorrected, an Infraction can lead to security violations or compromises. It requires an inquiry to facilitate immediate corrective action but does not require an in-depth investigation.

Violations are security incidents that indicate knowing, willful, and negligence for security regulations, and result in, or could be expected to result in, the loss or compromise of classified information. Security violations require an inquiry and/or investigation.

An Inadvertent Disclosure is the involuntary unauthorized access of classified SAP or unclassified HVSACO information to an individual without SAP access authorization.

Always safeguard SAP information involved in a possible security incident and report as required by DoDM 5205.07 V1.

Have a great day, and remember, be secure out there.

ENCLOSURE 8, pg. 34
SECURITY INCIDENTS AND INQUIRIES

To ensure the protection of classified information to include classified information protected by SAPs, security incidents will be investigated and actions will be taken to ensure that the adverse effects of loss or compromise of classified information are mitigated. Security incidents involving classified information will be handled and investigated in accordance with this manual and References (b) and (u).

a. All security violations will be reported immediately, to the extent possible, and no later than 24 hours of discovery, to the PSO, through the procedures described in this enclosure.

b. The PSO, through the chain of command, will advise the CA SAPCO in all instances where national security concerns would impact any security program or personnel security clearances (PCL) of SAP-accessed individuals. The PSO will notify and report security violations to the GPM with a copy of the report to the appropriate CA SAPCO. The security official of the affected SAPF will recommend the scope of the corrective action taken in response to the violation and report it to the PSO for approval.

c. Actual or potential compromises involving DoD SAPs, the results of the compromise or inquiries, and investigations that indicate weaknesses or vulnerabilities in establishing SAP policy, or procedures that contributed to an actual or potential compromise will be reported to the CA SAPCO, Original Classification Authority, and the DoD SAPCO, who will report to the Director of Security Policy and Oversight, Office of the USD(I).

d. Personnel determined to have had unauthorized or inadvertent access to classified SAP information:

(1) Will be interviewed by the GSSO, CPSO, or PSO to determine the extent of the exposure.

(2) May be requested to complete an inadvertent disclosure statement. An inquiry will be conducted to determine the circumstances of the inadvertent disclosure.

e. Guard personnel or local emergency authorities (e.g., police, medical, fire) inadvertently exposed to SAP material during an emergency response situation will be interviewed by the GSSO, CPSO, or PSO to determine the extent of the exposure.

(1) The PSO will determine if an inquiry is required by Reference (u) to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had, or could have had, access to the information.

(2) The inquiry identifies the facts, characterizes the incident as an infraction or a violation, and identifies, if possible, the cause(s) and person(s) responsible, reports corrective action or a requirement for an investigation.

f. Refusal to sign an inadvertent disclosure statement by personnel inadvertently exposed to classified information will be reported by the GSSO or CPSO to the PSO by the next duty day.

For each scenario, select the best answer. Check your answers in the Answer Key that follows the activity.

Scenario 1: Phone Call

Your phone rings. When you answer it, you hear: "This is Ms. Brown at the reception desk. A package was just dropped off for you. Oh, by the way, it's marked Secret."

When you retrieve the package, Ms. Brown explains that it was just delivered by U.S. Registered Mail. Upon opening the outer wrapper in the mailroom, she noted the inner wrapper was stamped Attn: Security Office and marked Secret//SAR-Red Train, so she immediately called you. The inner wrapper shows no evidence of tampering. She was the only employee in the mailroom when the outer wrapper was opened.

What type of security incident, if any, does this situation present?

a. A security violation
b. A security infraction
c. Not a security incident

Now that you know what kind of security incident you are dealing with, what is your next course of action? Select all that apply.

a. Report a security infraction to the CPSO/GSSO/PSO as appropriate within 24 hours
b. Open the package and determine that it does contain classified SAP materials
c. Document the infraction and make available to PSO during next visit
d. Don't contact the PSO, just secure the materials
e. Contact sender and remind them of your classified mailing address

Scenario 2: Email Notification

You have a new email. When you open the email attachment, you see that it is marked Secret//SAR- Wagon.

What type of security incident, if any, does this situation present?

a. A security violation
b. A security infraction
c. Not a security incident

Now that you know what kind of security incident, if any, you are dealing with, what is your next course of action? Select all that apply.

a. Forward the message to the PSO
b. Obtain cleanup action instructions from the PSO before taking any other action on the information system
c. Hit reply and let the sender know the message was sent over the wrong system
d. Delete the message
e. Report a security violation to the CPSO/GSSO/PSO as appropriate within 24 hours

Scenario 3: Access Badge

During a trip to the second floor break room, you discovered a security access badge lying on the counter. Upon inspection, you see it belongs to your coworker Raul Gonzalez.

What type of security incident, if any, does this situation present?

a. A security violation
b. A security infraction
c. Not a security incident

Now that you know what kind of security incident, if any, you are dealing with, what is your next course of action? Select all that apply.

a. Call the PSO and report a found badge
b. Turn the badge into lost and found on the first floor
c. Find the badge owner's phone extension in the company directory and let him know you found his badge
d. Contact facility security

Scenario 4: Forgotten Folder

You find a file folder on your chair when you return to your desk. It has a post-it note attached to the front reading:

First floor receptionist said you left this on her desk and asked me to give it to you.
-John

You open the folder and recognize the material. It's stamped Unclassified//HVSACO. You must have left it at the receptionist's desk when you picked up that package earlier.

What type of security incident, if any, does this situation present?

a. A security violation
b. A security infraction
c. Not a security incident

Now that you know what kind of security incident, if any, you are dealing with, what is your next course of action? Select all that apply.

a. Secure the information as appropriate
b. Do nothing. Since the information is Unclassified, the incident is not reportable.
c. Contact GSSO/PSO/CPSO by the next duty day to report inadvertent disclosure and obtain guidance on whether or not a preliminary inquiry is warranted
d. Keep quiet and maybe no one else will find out about this

Scenario 5: FAX

You pick up a document from the unclassified FAX machine. The FAX is marked Confidential//SAR-Red Train.

What type of security incident, if any, does this situation present?

a. A security violation
b. A security infraction
c. Not a security incident

Now that you know what kind of security incident, if any, you are dealing with, what is your next course of action? Select all that apply.

a. Report a security violation to the CPSO/GSSO/PSO as appropriate within 24 hours
b. Properly secure the SAP information
c. Shred the FAX
d. Write "This is not a secure FAX" on the FAX cover sheet and send the FAX back to the sender

Answer Key

Scenario 1: Phone Call

Your phone rings. When you answer it, you hear: "This is Ms. Brown at the reception desk. A package was just dropped off for you. Oh, by the way, it's marked Secret."

When you retrieve the package, Ms. Brown explains that it was just delivered by U.S. Registered Mail. Upon opening the outer wrapper in the mailroom, she noted the inner wrapper was stamped Attn.: Security Office and marked Secret//SAR-Red Train, so she immediately called you. The inner wrapper shows no evidence of tampering. She was the only employee in the mailroom when the outer wrapper was opened.

What type of security incident, if any, does this situation present?

a. A security violation
b. A security infraction
c. Not a security incident

Rationale: This is a security infraction. Because the package is securely wrapped there is no reason to suspect possible compromise (a security violation) or inadvertent disclosure. However, since the outer wrapper was opened in an unsecure area, this is a security infraction.

Now that you know what kind of security incident, if any, you are dealing with, what is your next course of action? Select all that apply.

a. Report a security infraction to the CPSO/GSSO/PSO as appropriate within 24 hours
b. Open the package and determine that it does contain classified SAP materials
c. Document the infraction and make available to PSO during next visit
d. Don't contact the PSO, just secure the materials
e. Contact sender and remind them of your classified mailing address

Rationale: Security infractions must be documented and made available for review by the PSO during visits. Opening the package and properly securing any SAP materials is also a sound security practice. You should also contact the sender to ensure this does not happen again.

Scenario 2: Email Notification

You have a new email. When you open the email attachment, you see that it is marked Secret//SAR- Wagon.

What type of security incident, if any, does this situation present?

a. A security violation
b. A security infraction
c. Not a security incident

Rationale: This is a security violation. While the information system is cleared for Secret information, the recipient is not cleared for Secret//SAR- Wagon.

Now that you know what kind of security incident, if any, you are dealing with, what is your next course of action? Select all that apply.

a. Forward the message to the PSO
b. Obtain cleanup action instructions from the PSO before taking any other action on the information system
c. Hit reply and let the sender know the message was sent over the wrong system
d. Delete the message
e. Report a security violation to the CPSO/GSSO/PSO as appropriate within 24 hours

Rationale: Do not reply or forward the message. This would only compound the violation. Do not delete the message. A record of the transmission may be needed for any investigation that may be conducted. You should contact the CPSO/GSSO/PSO as appropriate, report the security violation and await guidance on the appropriate cleanup procedures before taking any action on your information system.

Scenario 3: Access Badge

During a trip to the second floor break room, you discovered a security access badge lying on the counter. Upon inspection, you see it belongs to your coworker Raul Gonzalez.

What type of security incident, if any, does this situation present?

a. A security violation
b. A security infraction
c. Not a security incident

Rationale: Since the badge was found in the second floor break room within the SAP facility, this is not a security incident. Although the access badge was found in the second floor break room, within the SAP facility, personnel are still required to maintain positive control at all times.

Now that you know what kind of security incident, if any, you are dealing with, what is your next course of action? Select all that apply.

a. Call the PSO and report a found badge
b. Turn the badge into lost and found on the first floor
c. Find the badge owner's phone extension in the company directory and let him know you found his badge
d. Contact facility security

Rationale: Since this is not a security incident, contacting the badge owner and returning the badge is sufficient.

Scenario 4: Forgotten Folder

You find a file folder on your chair when you return to your desk. It has a post-it attached to the front reading:

First floor receptionist said you left this on her desk and asked me to give it to you.
-Simon

You open the folder and recognize the material. It's stamped Unclassified//HVSACO. You must have left it at the receptionist's desk when you picked up that package earlier.

What type of security incident, if any, does this situation present?

a. A security violation
b. A security infraction
c. Not a security incident

Rationale: Unclassified//HVSACO material was subject to involuntary unauthorized access by individuals without SAP access authorization. This is a security infraction.

Now that you know what kind of security incident, if any, you are dealing with, what is your next course of action? Select all that apply.

a. Secure the information as appropriate
b. Do nothing. Since the information is Unclassified, the incident is not reportable.
c. Contact GSSO/PSO/CPSO by the next duty day to report inadvertent disclosure/security violation and obtain guidance on whether or not a preliminary inquiry is warranted
d. Keep quiet and maybe no one else will find out about this

Rationale: While it may be difficult to report yourself, this is a security infraction that must be reported to the GSSO immediately. The GSSO is required to report to the PSO within 24 hours.

Scenario 5: FAX

You pick up a document from the unclassified FAX machine. The FAX is marked Confidential//SAR-Red Train.

What type of security incident, if any, does this situation present?

a. A security violation
b. A security infraction
c. An inadvertent disclosure
d. Not a security incident

Rationale: Because the FAX machine is only approved for Unclassified information and the FAX contains information that is Confidential//SAR-Red Train, this is a security violation.

Now that you know what kind of security incident, if any, you are dealing with, what is your next course of action? Select all that apply.

a. Report a security violation to the CPSO/GSSO/PSO as appropriate within 24 hours
b. Properly secure the SAP information
c. Shred the FAX
d. Write “This is not a secure FAX” on the FAX cover sheet and send the FAX back to the sender

Rationale: Do not return the FAX. This could compound the violation. Do not destroy the FAX. A record of the transmission may be needed in the event of an investigation. You should report a security violation and properly secure the information.

Conclusion

Good job identifying possible SAP security incidents. Remember to be vigilant and refer to DoD Special Access Program (SAP) Security Manual: General Procedures, DoD 5205.07, Vol.1 to help you identify SAP security incidents and reporting requirements.