Security Incidents Reporting Requirements Short

Student Guide

January 2025

Center for Development of Security Excellence

Contents

Opening

We've just received breaking news that classified information was leaked when a civilian government employee tweeted pictures of a Top Secret Report.

This incident where a classified document was found on an unauthorized electronic device, raises concerns about various security breaches that can lead to classified information being disclosed, such as an unsecured classified document left unattended, a classified document improperly transferred without following protocol, or classified information unwittingly sent over an unclassified network.

Protection of classified information is critical to national security, and prompt reporting of security incidents ensure that they are properly investigated, mitigated, and prevented from recurring.

This Short will review security incidents and the procedures for reporting requirements that must be implemented for different types of security incidents.

When you have completed this Short, you should be able to determine the appropriate reporting requirements to implement for a given security incident scenario.

Preventing Unauthorized Disclosure

As you just learned, a security incident can lead to disastrous consequences that impact the security of this nation.

In the news story you saw, classified information was leaked when a civilian government employee tweeted pictures of a Top Secret Report.

Each of the following scenarios represents ways that security incidents can lead to unauthorized disclosure of classified information.

- **Security Incident:** Unsecured Information
- **Security Incident:** Improper Transfer
- **Security Incident:** Spillage
- **Security Incident:** Unauthorized Device

Breaking news can erupt when classified or sensitive documents are left unattended in vulnerable locations, such as a conference room, public area, or unlocked office. There is a risk that unauthorized individuals could access the information.

Security Incident: Unsecured Information

Becky is employed by a government agency that works frequently with classified information on allied partner weapons systems. Her office and surrounding rooms are not approved for open storage and therefore, all classified information in these offices

must be protected at all times. Becky has a GSA-approved security container in her office and so do multiple other personal offices in her directorate.

Becky is at her desk, beginning to work on a new classified project, when she realizes that she left her coffee mug in the conference room during a meeting earlier in the day. As she retrieves her mug, she notices a folder on the table. Upon closer inspection, she notices that the exterior of the folder has no markings except for the title of the classified project that she is working on.

She opens the folder to see if she can tell who the owner is and quickly realizes that the inside document has classification markings. Becky is considered a subject matter expert on the information and has Secret eligibility, a signed non-disclosure agreement (NDA), a need to know, and Secret level access.

She decides to read the information to ensure it is indeed classified and marked appropriately. She sighs as she confirms what she feared. The information is in fact Secret. What should Becky do now?

Unsecured Information: Inquiry Official Tasks

Becky secures the document and immediately notifies her director and the activity security manager. Becky's activity security manager, Susan, thanks Becky for bringing the incident to her attention and then coordinates with the supervisor to appoint an inquiry official.

After careful evaluation of the current employees and their rank and grade, the supervisor selects Vera to conduct the inquiry. Vera first meets with her director, Danny, who is overseeing the incident to get briefed on her own responsibilities as the inquiry official.

She understands now that the primary objective is to ensure the protection of national classified information. If during her inquiry, she believes that a compromise of classified information occurred, she is to immediately report it to Danny.

Unsecured Information: Building the Inquiry

Her next stop is to meet with the responsible security manager, Susan. Susan briefs Vera on her specific duties and the required contents of the final report referenced in DOD Manual, or DODM 5200.01, Volume 3, which includes: Summary, Sequence of Events, Actions Taken, and Recommendations.

Unsecured Information: Outcome

Vera can now conduct an inquiry to identify the facts.

Inquiry

An inquiry into an incident determines if classified information is unaccounted for or if unauthorized personnel had, or could have had, access to the information. Visit the Resources for the Security Incident Inquiry Guide for information on how to conduct an effective inquiry.

Inquiry Findings

Becky secured the Secret document in a GSA-approved security container, so it is accounted for.

Vera spoke to everyone in the meeting with Becky. Included on her project team was an analyst, Flora, with authorized access that happens to sit outside the conference room.

Becky's colleague Ted left the document behind by mistake. Flora confirmed that no one had been in the conference room since the meeting ended.

Vera wants to confirm this and follows up with the Physical Security manager, Jon, to review the closed circuit camera footage outside the conference room for that time period. He is able to confirm no one accessed the room in the timeframe.

Vera now feels confident in her assessment that no one had been in the conference room since Becky's project meeting. She completes the inquiry report and delivers it to Danny for approval. At this point, the director can recommend additional recommendations before the inquiry is finalized.

Security Infraction

This security incident is an example of an infraction, which means that although there was a failure to comply with requirements there is no loss, compromise, or suspected compromise of classified information.

The activity security manager recommends refresher training on protecting and storing classified information for Ted as a corrective action.

Knowledge Check 1

What should you do if you find unsecured classified information?

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

- ☐ Safeguard the information.
- ☐ Take the document home to keep it safe until the next meeting.
- ☐ Leave the document where you find it in case the owner comes back for it.
- ☐ Immediately notify the commander or director and the activity security manager.

Knowledge Check 2

Which of the following are recommended elements to include in the final report of a security incident inquiry or investigation in accordance with DODM 5200.01, Volume 3?

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

- ☐ Summary
- ☐ Sequence of Events
- ☐ Actions Taken
- ☐ Security Container Serial Numbers
- ☐ Recommendations

Preventing Unauthorized Disclosure

Breaking news could also arise if classified documents are sent through non-secure channels, such as standard postal services, instead of approved secure couriers. There is a risk that the package could be intercepted, lost, or delivered to unauthorized recipients.

Security Incident: Improper Transfer

Josh is a contract analyst working at a government agency that focuses on US weapons sales and shipments to multiple foreign countries. Josh constantly receives packages from team members deployed overseas mostly containing unclassified reports.

Josh receives a package via USPS First Class from his activity security manager, who is currently deployed. He opens the package from his security manager thinking the package is no different than the countless others he has opened before. As Josh opens the package, he notices the inner wrapping is clearly marked "SECRET." However, he quickly realizes that the package was not sent through authorized channels, such as an

approved courier or a tracked, receipt-based system, as required for the transmission of classified materials. What should Josh do?

Improper Transfer: Inquiry Official Tasks

Since Josh believes that his activity security manager is responsible for improperly transferring the information, as an alternative he should report to the security authorities at the next higher level of command or supervision. Josh works in the Logistics Branch level, so he has multiple levels above him to include Eastern Division (one or next level higher) and the Middle East Center (two levels higher).

Or Josh could report to the commanding officer or security manager at the most readily available DOD facility. Alternatively, Josh could report to DOD law enforcement, counterintelligence (CI), or defense criminal investigative organization (DCIO).

Josh happens to know the Eastern Division Chief, Jovanna, who used to be a security manager herself. He decides that is the best course of action for reporting the incident, since she is in a director position at the next higher level. Jovanna thanks Josh for reporting the incident and decides to appoint someone of appropriate rank and grade from one of the co-located Air Force units as the inquiry official after coordinating with the Air Force director at that unit.

Eric, the appointed inquiry official, is an Air Force civilian and reports to Jovanna to fully understand his responsibilities as the inquiry official. He understands now that the primary objective is to ensure the protection of classified national security information. If during his inquiry, he believes that a compromise of classified information occurred, he is to immediately report it to Jovanna.

Improper Transfer: Outcome

Jovanna briefs Eric on the sensitivities surrounding the current activity security manager's involvement in the incident and directs him to her own supporting activity security manager, Jessica, to discuss his inquiry official duties in greater detail.

Jessica briefs Eric on his specific duties and the recommended contents of the final report referenced in DODM 5200.01, Volume 3, which includes Summary, Sequence of Events, Actions Taken, and Recommendations.

After Eric meets with the security team and reviews the logistics handling software logs that track shipments and packages, he determines that this security incident is a violation.

A violation indicates negligence for security regulations that resulted in, or could result in, a loss, compromise, or potential compromise of classified information.

The transmission of classified information by an unapproved means (USPS First Class in this specific case) is an example of a special circumstance and is considered a compromise of classified information.

To learn more about specific circumstances that require unique handling or consideration of additional reporting requirements in accordance with DODM 5200.01, Volume 3, refer to the Special Types of Security Incidents job aid available through the Resources.

This violation requires an in-depth and comprehensive investigation to assess whether classified information was compromised during transit.

Knowledge Check 3

In a security incident where an activity security manager is believed to be involved, what should you do if you believe that classified information has been transferred improperly?

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

- ☐ Open the inner wrapping immediately.
- ☐ Dispose of the package.
- ☐ Notify the security authorities at the next higher level of command/supervision.
- ☐ Safeguard the information.

Preventing Unauthorized Disclosure

Breaking news could quickly unfold if a spillage of classified information occurs. Spillage refers to the accidental or intentional transfer of classified information to an unauthorized or unclassified environment, such as sending classified data via an unsecure email system or storing it on a network that with a lower level of classification, or to a system not accredited to process data of that restrictive category.

Security Incident: Spillage

Nick is an Army civilian that works in the G5 Plans directorate at an Army Division level headquarters. He is currently working on updating the Continuity of Operations Plan (COOP) for his installation.

Most of the plan is unclassified, but a small portion of the plan is considered classified and must be coordinated on classified systems such as the Secret Internet Protocol Router Network (SIPR) network on his base.

Nick has just started his day and decides to work through some emails before diving back into the COOP update. He opens one email from a member on his team that is also working on the plan. His teammate is asking questions and giving suggested answers that should be addressed at the next COOP coordination session.

Nick receives the email over an unclassified network, or Non-Classified Internet Protocol Router Network (NIPRNet). However, he realizes as he reads the questions and potential answers to be addressed in the session that the email inadvertently reveals Secret classified information through compilation. He quickly reviews the Security Classification Guide that covers the COOP and realizes his classification by compilation suspicion is correct. Classification by compilation occurs when two or more pieces of unclassified information when combined disclose classified information. What should Nick do?

Spillage: Official Tasks

This is an example of spillage, because Secret classified information has been inadvertently transmitted over an unclassified network, which violates security protocols.

Nick recognizes that excerpts from the Security Classification Guide he was just reviewing indicate that the elements mentioned in the email, when combined, are classified by compilation.

Nick is certain spillage has occurred, because the email contains a combination of elements that, when compiled, reveal classified information. He immediately reports the incident to his director and the activity security manager.

Nick does not delete, forward, or manipulate the file. He secures the area and immediately notifies Mary, the director and Phil, the activity security manager.

Phil coordinates with Mary, the information technology (IT) team, and the Information Systems Security Manager (ISSM), Kyle, to ensure the necessary requirements are completed.

Spillage: Building the Inquiry

Kyle works with IT to remove the classified information from the unclassified email system to prevent further spread. Mary appoints Carrie as the Inquiry Official to conduct the inquiry, notify any required parties, conduct an investigation if the result of the inquiry requires it, and perform a damage assessment.

Damage Assessment

A damage assessment involves a detailed review of the facts surrounding the compromise of classified information to determine its impact on DOD programs, operations, and capabilities. This includes assessing practical effects, implementing mitigations, and estimating costs to restore security or replace compromised systems. The assessment typically follows a classification review and may occur after any legal proceedings, although it can be done pre-prosecution if needed. It differs from immediate damage control actions and the classification review conducted by the Original Classification Authority (OCA). DOD components are required to conduct damage assessments, especially in cases of espionage, intelligence breaches, or media leaks. The OCA and subject matter experts are responsible for these assessments, aided by security officials. Information from related security inquiries or investigations may be used to support the damage assessment. See Enclosure 6, Section 10 of DODM 5200.01, Volume 3 to learn more.

Outcome: Spillage

As required by DOD policy, in accordance with DODM 5200.01, Volume 3, the Army has procedures in place to remediate up to Secret-level spills.

The cybersecurity team quickly implements technical isolation of contaminated workstations, servers, and back-up systems to avoid widespread contamination, and begins the process of determining whether an unauthorized disclosure occurred.

The cybersecurity team reviews system audit logs that track who received, opened, or forwarded the email and determine that only Nick opened the email. Nick's system was sanitized, and it was determined that an unauthorized disclosure of classified information did not occur.

Knowledge Check 4

Which of the following actions should be taken to secure classified information after a spillage?

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

- ☐ Notify appropriate authorities.
- ☐ Delete any electronic evidence related to the spillage.
- ☐ Isolate and preserve all materials involved in the spillage.
- ☐ Allow other employees to continue working in the area.

Preventing Unauthorized Disclosure

Breaking news could rapidly develop if a Prohibited Personal Electronic Device (PED) is introduced into a secure environment, leading to potential breaches of classified information. The use of personal smartphones, laptops, or USB drives can create pathways for sensitive data to be accessed or transmitted without proper security measures, resulting in significant risks to national security.

Security Incident: Prohibited Personal Electronic Devices

Pam is a Navy civilian working as an intelligence analyst at a Navy advanced warfighting school. She splits her time working either in a collateral secure area and a Sensitive Compartmented Information Facility (SCIF).

Her team works on enemy tactics, techniques, and procedures (TTPs) and developing US Navy TTPs in order to counter them. Pam walks into a designated secure area where sensitive information is handled and observes her colleague, Alex, taking pictures with his smartphone of a Top Secret Report that is being prepared for transmission to the Director of Operations. What should Pam do?

Prohibited Personal Electronic Devices: Building the Inquiry

Pam immediately reports the incident to her director, Oliver, who coordinates with the activity security manager Jeff to appoint an inquiry official. The inquiry official Kenny conducts the inquiry, and interviews the witnesses, Pam and Mark.

Outcome: Prohibited Personal Electronic Devices

The Navy cybersecurity team members extract data from Alex's phone and confirm that the phone's contents were uploaded to social media sites. These sites were found to have multiple unauthorized social media contacts commenting on the member's classified posts, including multiple foreign entities.

Pam's security officials recognize that this is an egregious security incident and a clear security violation because classified information has been compromised. Security incidents of this nature require notification to the Director of Security, Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)).

Additionally, if the information that was compromised in this incident relates to any defense operation, system, or technology, other reporting is required. For information on what to report, who reports, and special circumstances reference DODM 5200.01, Volume 3, Enclosure 6, Reporting and Notifications and the Reporting Guidelines job aid in Resources.

Knowledge Check 5

Pam's security officials consider this incident an egregious security violation because classified information was compromised, unauthorized contacts were involved, and foreign entities were part of the incident. In addition to standard reporting, which of the following is required for egregious security violations?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

- ○ Notification to the Secretary of Defense
- ○ No further action is needed.
- ○ Notification to the Director of Security, Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S))
- ○ Immediate destruction of the compromised information

Classification of Reports

Security incident reports must be classified according to the report's contents and as outlined in the applicable security classification guides. At a minimum, the report must be designated as Controlled Unclassified Information (CUI). This minimum marking requirement helps to protect from any further unauthorized disclosure of protected information.

If the lost or compromised information cannot be recovered, such as in the case of a media leak, public website posting, or loss in a foreign country, the report and location of the compromise must be classified at the level of the compromised material to prevent further unauthorized disclosure.

Lessons Learned

These types of scenarios, whether a leaked classified report via social media, an improper transfer, or another form of unauthorized disclosure, can cause serious national security breaches. Each incident highlights the critical importance of following proper security protocols and swiftly reporting any violations.

Conclusion

As you've learned, it is critical to safeguard classified information and promptly report security incidents involving classified information.

All security incidents involving classified information will result in a security inquiry.

When a security incident cannot be resolved via inquiry, a security investigation or more in-depth examination is necessary to resolve the incident.

A security incident will be categorized as an infraction when it involves the failure to comply with requirements but does not result in the loss, suspected compromise, or actual compromise of classified information.

A security incident will be categorized as a violation when failure to comply with requirements results in the loss, compromise, or potential compromise of classified information.

Congratulations. You have completed the Security Incidents Reporting Requirements Short. In this Short, you learned how to evaluate specific security incident scenarios and determine the reporting requirements to implement in accordance with regulatory guidance.

Visit the Resources for the Special Types of Security Incidents Job Aid.

Appendix A: Answer Key

Knowledge Check 1

What should you do if you find unsecured classified information?

- ☑ Safeguard the information. [correct response]
- ☐ Take the document home to keep it safe until the next meeting.
- ☐ Leave the document where you find it in case the owner comes back for it.
- ☑ Immediately notify the commander or director and the activity security manager. [correct response]

***Feedback**: First safeguard the information, then immediately notify the commander or director and the activity security manager.*

Knowledge Check 2

Which of the following are recommended elements to include in the final report of a security incident inquiry or investigation in accordance with DODM 5200.01, Volume 3?

- ☑ Summary [correct response]
- ☑ Sequence of Events [correct response]
- ☑ Actions Taken [correct response]
- ☐ Security Container Serial Numbers
- ☑ Recommendations [correct response]

***Feedback**: The Summary, Sequence of Events, Actions Taken, and Recommendations are recommended elements to include in the final report for a security incident inquiry or investigation in accordance with DODM 5200.01, Volume 3.*

Knowledge Check 3

In a security incident where an activity security manager is believed to be involved, what should you do if you believe that classified information has been transferred improperly?

- ☐ Open the inner wrapping immediately.
- ☐ Dispose of the package.
- ☑ Notify the security authorities at the next higher level of command/supervision. [correct response]
- ☑ Safeguard the information. [correct response]

***Feedback**: In a security incident where an activity security manager is believed to be involved, you should safeguard the information first, and then notify the security authorities at the next higher level of command/supervision.*

Knowledge Check 4

In a security incident where an activity security manager is believed to be involved, what should you do if you believe that classified information has been transferred improperly?

- ☑ Notify appropriate authorities. [correct response]
- ☐ Delete any electronic evidence related to the spillage.
- ☑ Isolate and preserve all materials involved in the spillage. [correct response]
- ☐ Allow other employees to continue working in the area.

***Feedback**: To secure classified information after a spillage, you should notify the appropriate authorities and isolate and preserve all materials involved in the spillage.*

Knowledge Check 5

Pam's security officials consider this incident an egregious security violation because classified information was compromised, unauthorized contacts were involved, and foreign entities were part of the incident. In addition to standard reporting, which of the following is required for egregious security violations?

- ○ Notification to the Secretary of Defense
- ○ No further action is needed.
- ⊙ Notification to the Director of Security, Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) [correct response]
- ○ Immediate destruction of the compromised information

***Feedback**: Because this incident is considered an egregious security violation, the Director of Security, Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) should be notified in addition to standard reporting procedures.*