Student Guide

Short: Security Incidents Reporting Requirements

Objective	Identify the appropriate reporting requirements to follow in the event of a security incident.
Estimated completion time	10 minutes

Reporting a Security Incident

It began as another ordinary day at the office. Tom grabbed a cup of coffee and got to work. As he printed out the latest project report, he discovered a classified document sitting on the printer. Looks like it wasn't going to be such an ordinary day after all.

What is the first thing Tom should do about the Secret document on the printer tray? Select the best response.

- ○ Notify the head of his local activity.
- ○ Notify the activity security manager.
- ○ Take control of the document.

Additional Reporting Considerations

In addition to finding classified material out of proper control, any known loss or potential compromise of classified information should be reported to the head of the local activity and to the activity security manager. But what if these individuals are believed to be involved in or responsible for the incident?

Who should you report a security incident to if you suspect the security authorities of your activity are involved or responsible? Select the best response(s).

- ☐ Notify the security authorities at the next higher level of command/supervision.
- ☐ Notify commanding officer or security manager at the most readily available DoD facility.
- ☐ Notify your activities security authorities regardless of who is involved.

After an Incident Report

Having secured the classified documents, Tom immediately notifies the proper security officials. Tom's security manager, Jane, thanks him for bringing the incident to her attention and indicates that she will be initiating an inquiry to identify the facts, the causes, and the person responsible in order to determine if the incident is an infraction or a violation.

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. In addition to identifying the facts and type of incident, an inquiry includes recommendations about the corrective actions to be taken.

Infraction

The classification of a security incident as an infraction means that there was a failure to comply with requirements where there is no loss, compromise or potential for compromise.

Non-compliance

The classification of a security incident as a violation indicates a knowing and willful negligence for security regulations that resulted in, or could be expected to result in, a loss, compromise or potential compromise of classified information. In such a case, an inquiry must be conducted in order to provide an in-depth and comprehensive examination of the matter.

Significant Consequences

The initial inquiry revealed that the classified document was missing some pages. The document contained information concerning a Secret defense technology which will likely cause an adverse effect to national security. What needs to happen now?

What's the next step concerning the loss of classified information related to a defense technology? Select the best response.

- ○ Confer with the head of the local activity in order to identify recommendations for corrective actions to implement.
- ○ Complete the required Security Incident Report and notify the next higher level of command/supervision.
- ○ Report the violation to the Director of Security at the OUSD(I)

Reporting Requirements for the Director of Security, OUSD(I)

Any incident that results in, or may result in, significant consequences or may become public must be promptly reported to the Director of Security at the Office of the Under Secretary of Defense for Intelligence, or OUSD(I). A preliminary report should be included especially if the incident could become public.

Incidents that require reporting include any egregious security incident as determined by the DoD Component senior agency official or violations:

- Involving espionage
- Resulting in an unauthorized disclosure of classified information to the public media
- Involving disclosure that:
  - Is reported to a Congressional oversight committee
  - May attract significant public attention
  - Involves large amounts of classified information
  - Reveals a potential systemic weakness in policy or practices
- Involving the creation or continuation of a SAP contrary to regulation requirements and national policies
- Relating to any defense operation, system, or technology that is likely to cause significant harm or damage to national security

Summary

Reporting ensures that the oversights that led to security incidents are corrected. As such, reports need to be available for inspection, analysis, review, and/or investigation. To assist in doing this, reports need to be filed using the Security Incident Report module of the Operations Security Collaboration Architecture, or OSCAR. Dependent on the nature of the incident, there may be additional reporting requirements to consider.

When it comes to reporting a security incident, the most important thing to remember is the immediacy of the situation. By reporting incidents to the proper officials in a timely manner, you help to ensure the integrity of national security.

Answer Key

What is the first thing Tom should do about the Secret document on the printer tray? Select the best response.

- ○ Take control of the document.

Who should you report a security incident to if you suspect the security authorities of your activity are involved or responsible? Select the best response(s).

- ☐ Notify the security authorities at the next higher level of command/supervision.
- ☐ Notify commanding officer or security manager at the most readily available DoD facility.

What's the next step concerning the loss of classified information related to a defense technology? Select the best response.

- ○ Report the violation to the Director of Security at the OUSD(I)