CDSE

Security Incident Inquiry Guide

Inquiry: An inquiry is fact-finding and analysis conducted to determine whether there was a loss of classified or even the potential for loss of classified information, or whether unauthorized personnel had, or could have had, access to the information. To conduct an effective inquiry, you need to answer six questions.

1. Who?

- Who was involved?
- Did the discoverer read the information?
- Have they been properly briefed?

2. What?

- What are the specific details regarding the incident?
- What information was possibly lost or compromised?
- What are the specific details regarding the incident?
- What information was possibly lost or compromised?

3. When?

- What is the date and time of the incident?
- Was it the end of the day, lunch time, first thing in the morning, or the weekend when no one else was around?

4. Where?

- What is the specific location and address where the incident occurred?
- Was the information left in a conference room, rest room or an unauthorized person's desk?

5. Why?

- Was the incident intentional or inadvertent?
- Was it due to poor training?
- Did the person have a lack of respect for security procedures or were they unaware?

6. How?

- Can you explain or determine exactly how the incident occurred?
- How long was the information vulnerable to potential loss or compromise?

Incident Reporting

If the inquiry determines that an actual loss or compromise occurred, then the official initiating the inquiry must notify the Original Classification Authority (OCA) for the compromised information.

Other officials must be notified outside your environment if the incident falls into special circumstances, which requires unique handling or additional reporting requirements. If the inquiry determines NO compromise occurred, then you or the inquiry official must determine why or how the security incident occurred:

- Did the involved person(s) fail to comply with established security practices and procedures?
- Was it intentional or unintentional?
- Is there a weakness or vulnerability in established security practices and procedures?
- Should changes be made to the process or activity's security program?

Ten duty days are allowed to complete an inquiry. If the inquiry cannot be completed within 10 duty days, an extension should be requested from the appointing official.