Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

# Security Incident Requirements

## Information Security Webinar

CDSE

### Security Incident Requirements

**Host:** Lisa Rainey, SAPPC

Information Security Curriculum Manager, DSS - CDSE

- Distinguished career-security professional
- Security Asset Protection Professional Certification (SAPPC)
- Retired US Army
- Security Manager/Antiterrorism Officer
- Physical Security Program management
- Personnel Security Program management
- Mobilization/Readiness management
- OPSEC Officer
- Contracting Officers Representative

03/21/2013

## Administrative Announcements

CDSE

- **Use the Q & A box to ask questions.**
- **These slides can be downloaded. Select the file in the File Share box below.**
- **Enclosure 6 of Volume 3 DoD Manual 5200.01 is also provided in the File Share box.**
- **This webinar will present poll questions.**

## Poll 1

## DoDM 5200.01, Vol 3, Encl. 6


Department of Defense
MANUAL

Personnel have a responsibility to:

- Promptly report security incidents
- Ensure incidents are properly investigated
- Minimize adverse effects of unauthorized disclosure
- Preclude recurrence through education

## Common Sense Approach

- If no adverse effect on national security, resolve at lowest appropriate level.
- Any incident involving classified information must involve an inquiry and/or investigation.

## Compromise vs. Loss

**COMPROMISE**
Security Incident (Violation)
Unauthorized Disclosure

**LOSS**
Missing Classified Information/Equipment

## Chat Question

**When would a security incident require an investigation?**

Enter your responses in the chat box.

## Security Violation

- **Unauthorized Disclosure**
- **Misclassification**
- **Continue or discontinue a SAP**
- **Anything else outside of Manual requirements**
- **Requires an *inquiry, investigation, or both***

Actual or Potential loss or compromise of classified information

**Administrative in Nature**

**Negligent** | **Willful** | **Knowing**

## Security Infraction

- Failure to comply with DoDM 5200.01 or other policy
- Does not result in loss, suspected compromise, or compromise
- May be unintentional or inadvertent
- Does not require an in-depth investigation

If the incident does not fit under the violation categories below, it is an infraction.

Administrative in Nature

Negligent | Willful | Knowing

## Inquiry

- Identifies the facts
- Determines infraction or violation
- Identifies possible causes and person(s) responsible
- Reports corrective actions
- Makes recommendations for further action or investigation

## Investigation

Conduct an investigation if the inquiry does not resolve all issues.

## Security Tips

Dangerous practices:
- Recycling box next to copier
- Burn bags next to unclassified trash containers
- Personal business during hand-carrying
- Failing to change security container combinations

## Poll 2

## Consequences of Compromise

After a compromise occurs:
- Regain custody of compromised material
- Identify source and reason
- Take remedial action

## Reporting and Notifications

- Must be safeguarded
- Notify, using secure communications
- If necessary, report to authorities at next higher level.

## Reporting

Notify Director of Security, OUSD(I) of:

- Espionage
- UD to public media
- Establishment or continuance of a SAP
- Compromise likely to cause significant damage

Con't

## Reporting, con't

Also report violations involving:

- Knowing, willful, or negligent unauthorized disclosure
- Potential for attracting significant attention
- Large amounts of information
- Potential weakness in classification policies

## Classification of Reports


- At minimum, designate reports FOUO
- Classify commensurate with level of compromised material
- If disseminated outside of DoD, use an expanded marking

## Inquiries and Investigations

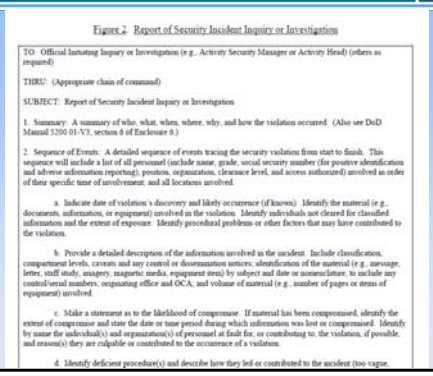

Figure 2. Report of Security Incident Inquiry or Investigation

TO: Official Initiating Inquiry or Investigation (e.g., Activity Security Manager or Activity Head) (others as required)

THRU: (Appropriate chain of command)

SUBJECT: Report of Security Incident Inquiry or Investigation

1. Summary: A summary of who, what, when, where, why, and how the violation occurred. (Also see DoD Manual 5200.01-V3, section 6 of Enclosure 6.)

2. Sequence of Events: A detailed sequence of events tracing the security violation from start to finish. This sequence will include a list of all personnel (include name, grade, social security number (for positive identification and adverse information reporting), position, organization, clearance level, and access authorized) involved in order of their specific time of involvement, and all locations involved.

a. Indicate date of violation's discovery and likely occurrence (if known). Identify the material (e.g., documents, information, or equipment) involved in the violation. Identify individuals not cleared for classified information and the extent of exposure. Identify procedural problems or other factors that may have contributed to the violation.

b. Provide a detailed description of the information involved in the incident. Include classification, compartment levels, caveats and any control or dissemination notices; identification of the material (e.g., message, letter, staff study, imagery, magnetic media, equipment item) by subject and date or nomenclature, to include any control/serial numbers; originating office and OCA; and volume of material (e.g., number of pages or items of equipment) involved.

c. Make a statement as to the likelihood of compromise. If material has been compromised, identify the extent of compromise and state the date or time period during which information was lost or compromised. Identify by name the individual(s) and organization(s) of personnel at fault for, or contributing to, the violation, if possible, and reason(s) they are culpable or contributed to the occurrence of a violation.

d. Identify deficient procedure(s) and describe how they led or contributed to the incident (too vague,

## Suspicion of Criminal Activity

**If criminal activity is suspected:**

- Inquiry and investigation ceases
- Begin coordination with cognizant DCIO or Defense CI component
- Continue inquiry or investigation if jurisdiction is declined

## Coordination with OCA

If it is determined that a compromise occurred:

- The originator (OCA) is notified.
- If the OCA no longer exists, or the inheriting activities cannot be determined, the DoD Component of the OCA shall be notified.
- The notification should not be delayed pending further investigation or resolution.

## Security Inquiries

Inquiry actions:

- Complete an inquiry in fewer than 10 duty days
- Report findings to activity head, activity security manager, and others as appropriate
- Request extension, if needed

## Security Inquiries, con't


Inquiry Report:

- Punitive action not recommended
- Prevention actions documented

Discipline is the responsibility of appropriate military commander or management official.

## Security Investigations

Conduct an investigation if the inquiry does not resolve all of the issues.

**The Investigator…**

Is a disinterested person

Has appropriate clearance and access

Has the ability to conduct an effective investigation

## Information Appearing in the Public Media

DoD personnel must not:
- Confirm or verify information
- Discuss with anyone who does not have appropriate clearance

Workforce may need to be reminded of actions to be taken or not taken in response to the disclosure.


## Results of Inquiries and Investigations

**Compromise Occurred**

Responsible security official issues revised guidance as necessary.

If there are defects in the procedures and requirements of the Manual, report to Director of Security, OUSD(I).

**Compromise did not Occur**

Responsible security official takes action as appropriate to resolve incident and/or failures to comply with procedures.

Notification to OCAs will not be delayed pending completion of additional investigations.

## Poll 3

## Compromises involving more than one Agency

Affected activities are responsible for coordinating their efforts in assessing damage.

## Debriefing in Cases of Unauthorized Access

- The activity head shall determine if a debriefing is warranted.
- A nondisclosure agreement (SF 312) may be executed.

## Reporting and Oversight Mechanisms


- Timely and efficient reporting and oversight
- Eliminate the probability of further incidents
- Simple disciplinary action is not an acceptable response to a security incident.

## Contacts and Resources

- Slides and frequently asked questions from this webinar will be posted at http://www.cdse.edu/catalog/webinars/information-security/security-incident-requirements.html
- Email information security training related questions to DSS at informationsecurity.training@dss.mil