# CHAPTER 10

# ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

## 10-100 Policy

a. The compromise of classified information can present a threat to the national security. Once a compromise is known to have occurred, the seriousness of damage to U.S. interests must be determined and appropriate measures taken to negate or minimize the adverse effect of such compromise. When possible, action also should be taken to regain custody of documents or material that were compromised. In all cases, appropriate action must be taken to identify the source and reason for the actual or potential compromise and remedial action to be taken to prevent recurrence.

b. Actual or potential compromises involving cryptologic information shall be handled in accordance with NACSI 4006.

c. Actual or potential compromises involving SCI will be handled in accordance with DoD S-5105.21-M-I.

## 10-101 Reporting

a. Anyone finding classified material out of proper control shall take custody of and safeguard the material, if possible, and immediately notify the appropriate security authorities.

b. Any person who becomes aware of the possible compromise of classified information shall immediately report it to the head of his or her local activity or to the activity security manager. If the person believes that the head of the activity or the security manager may have been involved in the incident, he or she may report it to the security authorities at the next higher level of command or supervision.

c. If classified information appears in the public media, DoD personnel must be careful not to make any statement or comment that would confirm the accuracy or verify the classified status of the information. Report the matter as instructed by the appropriate DoD Component directives, but do not discuss it with anyone without an appropriate security clearance and need-to-know. If approached by a representative of the media who wishes to discuss information you believe is classified, neither confirm nor deny the accuracy of or the classification of the information, and report the situation immediately to the appropriate security and public affairs authorities.

d. Any incident in which deliberate compromise of classified information or involvement of foreign intelligence agencies is suspected as well as apparent violations of criminal law shall be reported in accordance with DoD Instruction 5240.4. The Principal Director, Information Warfare, Security, and Counterintelligence (PD(IWSCI)); OASD(C3I), is the focal point for investigative matters involving the actual or potential compromise of classified information directed to the Department of Defense by other government agencies or that may involve other government agencies.

e. Local security officials will advise their parent command security officials of compromises occurring within their security cognizance and involving personnel assigned to that parent command.

f. If the head of an activity or the activity security manager to whom an incident is initially reported does not have security cognizance over the incident, such official shall ensure that the incident is reported to the appropriate authority. The organization with security cognizance shall ensure that an inquiry/investigation is conducted consistent with this chapter and for taking corrective action as required.

g. All compromises involving computer systems, terminals, or equipment shall be reported through appropriate channels to the Director, Information Assurance, Office of the Deputy Assistant Secretary of Defense (Command, Control and Communications) (DASD(C3)).

h. Compromises involving foreign government information shall be reported to the Director of International Security Programs, OUSD(P), who shall notify the foreign government.

i. Compromises involving DoD Special Access Programs, or results of inquiries/investigations that indicate that weaknesses or vulnerabilities in established SAP policy and/or procedures contributed to a potential compromise, shall be reported to the Director, Special Programs, OUSD(P).

j. Results of inquiries/investigations into actual or potential compromises that indicate that defects in the procedures and requirements of this Regulation contributed to the incident shall be reported to the PD(IWSCI), OASD(C3I).

10-102 Inquiry/Investigation

a. Preliminary Inquiry. When an actual or potential compromise of classified information occurs, the head of the activity or activity security manager having security cognizance shall promptly initiate an inquiry into the incident to determine the following. If information obtained as a result of the preliminary inquiry is sufficient to provide answers to these questions, then such information shall be sufficient to resolve the incident to include institution of administrative sanctions under Section 5, Chapter 1 of this Regulation:

(1) When, where, and how did the incident occur? What persons, situations, or conditions caused or contributed to the incident?

(2) Was classified information compromised?

(3) If a compromise occurred, what specific classified information and/or material was involved?

(4) If classified information is alleged to have been lost, what steps were taken to locate the material?

(5) In cases of compromise of classified information to the public media, the inquiry should determine:

(a) In what specific medial article or program did the classified information appear?

(b) To what extent was the compromised information disseminated?

(c) Was the information properly classified?

(d) Was the information officially released?

(6) If there was no compromise, was there a failure to comply with established security practices and procedures that could lead to compromise if left uncorrected and/or, is there a weakness or vulnerability in established security practices and procedures that could result in a compromise if left uncorrected? What corrective action is required?

b. Investigation. If the circumstances of an incident as such that a more detailed investigations is necessary, then an individual will be appointed to conduct that investigation. This individual must have an appropriate security clearance, have the ability to conduct an effective investigation, and must NOT be someone likely to have been involved, directly or indirectly, in the incident. Except in unusual circumstances, the activity security manager should not be appointed to conduct the investigation. In cases of compromise of classified information to the public media, the investigation should expand upon paragraph 10- 102a.5. above, to include:

(1) Are there any leads to be investigated that might lead to identification of the person responsible for the compromise?

(2) Will further inquiry increase the damage caused by the compromise?

10-103 **Results of the Inquiry/Investigation**

a. If the conclusion of the inquiry/investigation is that a compromise occurred, the official initiating the inquiry/investigation shall immediately notify the originator of the information or material involved. If the originating activity no longer exists, the activity that inherited the functions of the originating activity shall be notified. If the functions of the originating activity were dispersed to more than one other activity, the inheriting activity (ies) cannot be determined or, the functions have ceased to exist, the senior agency official of the DoD Component of which the originating activity was a part, shall be notified. This notification shall not be delayed pending completion of any additional inquiry/investigation or resolution of other related issues.

b. If the conclusion of the inquiry/investigation is that a compromise occurred and that a weakness or vulnerability in established security practices and/or procedures contributed to the compromise or that the potential exists for a compromise of classified information dues to a weakness or vulnerability in established security practices and/or procedures, the appropriate responsible security official shall take prompt action to issue new or revised guidance as necessary to resolve identified deficiencies.

c. If the conclusion of the inquiry/investigation is that a compromise did not occur but that there was potential for compromise of classified information due to a failure of a person or persons to comply with established security practices and/or procedures, the official having security cognizance over such persons or persons shall be responsible for taking action as may be appropriate to resolve the incident.

## 10-104 Verification, Reevaluation and Damage Assessment

a. When notified of the compromise of classified information or material, the original classification authority for that information or material shall:

(1) Verify the classification and duration of classification initially assigned to the information.

(2) Reevaluate the classification of the information to determine whether the classification should be continued or changed. This review should consider the following possibilities:

(a) The information has lost all or some of its sensitivity since it was initially classified, and should be downgraded or declassified. (In rare cases, it might also be discovered that the information has gained sensitivity, and should be upgraded.)

(b) The information has been so compromised by this incident that attempting to protect it further is unrealistic or inadvisable, and it should be declassified.

(c) The information should continue to be classified at its current level.

(3) Complete a damage assessment in accordance with DoD Instruction 5240.11.

b. While performing the reevaluation and damage assessment, the original classification authority must consider countermeasures that can be taken to minimize or eliminate the damage to the national security resulting from the compromise and then initiate or recommend adoption of such countermeasures. These countermeasures might include changing plans or system design features, revising operating procedures, providing increased protection to related information (through classification or upgrading), etc.

c. The verification, reevaluation and damage assessment process is to be completed as soon as possible following notification of a compromise. However, damage assessment requiring multi-disciplinary or multiple agency review of the adverse effects of the compromise on systems, operations, and/or intelligence, can sometimes be a long-term process.

d. When classified information under the control of more than one DoD Component or other agency is involved, the affected activities are responsible for coordinating their efforts in reevaluation and damage assessment.

## 10-105 Debriefings in Cases of Unauthorized Access

In cases where a person has had unauthorized access to classified information, it may be advisable to discuss the situation with the individual to enhance the probability that he or she will properly protect it. The activity head shall determine if a debriefing is warranted. This decision must be based on the circumstances of the incident, what is known about the person or people involved, and the nature of the classified information. The following general guidelines apply:

a. If the unauthorized access was by a person with the appropriate security clearance but no need-to-know, debriefing is usually appropriate only so far as necessary to ensure that the individual is aware that the information to which they had unauthorized access is classified and requires protection.

b. If the unauthorized access was by U.S. Government civilian or military personnel or an employee of a cleared U.S. Government contractor, without the appropriate security clearance, debriefing is usually appropriate. The person should be advised of their responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties that might follow if they fail to do so. The debriefing should be designed to ensure that the individual understands what classified information is, why its protection is important, and knows what to do should someone try to obtain the information. In the case of non-DoD personnel and employees of U.S. Government contractors, the appropriate security official in the individual's parent organization, to include the appropriate Facility Security Officer, should be advised of the debriefing.

c. If the person involved is neither member of a U.S. Government organization nor an employee of a cleared contractor, the decision is much more situational. The key question to be decided is whether the debriefing will have any likely positive effect on the person's ability or willingness to protect the information.

d. In any case where the person to be debriefed may be the subject of criminal prosecution or disciplinary action, consult with legal counsel before attempting to debrief the individual.

e. It is sometimes useful to have the person being debriefed sign a statement acknowledging the debriefing and his or her understanding of its contents. The nature and format of the statement is left to the discretion of the local security official so as to allow

flexibility in meeting the requirements of a particular incident. If the person refuses to sign a debriefing statement when asked, this fact and his or her stated reasons for refusing will be made a matter of record in the inquiry.

**10-106 Management and Oversight**

a. The DoD Components shall establish necessary reporting and oversight mechanisms to ensure that inquirieslinvestigations are conducted when required, that they are done in a timely and effective manner, and that appropriate management action is taken to correct identified problems. Inquiries/investigations and management analyses of security incidents must consider possible systemic shortcomings that may have caused or contributed to the incident. The effectiveness of activity security procedures, security education, supervisory oversight of security practices. etc., should be considered in determining causes and contributing factors. The focus of management response to security incidents should be to eliminate or minimize the probability of further incidents occurring. Appropriate disciplinary action or legal prosecution, discussed in Section 5 of Chapter 1, is sometimes one means of doing this, but the broader focus on prevention must not be lost. Simple disciplinary action—without consideration of what other factors may have contributed to the situation—should not be considered an acceptable response to a security incident.

b. Each DoD Component shall establish a system of controls and internal procedures to ensure that damage assessments are conducted when required and that their results are available as needed.

**10-107 Additional Investigation**

Additional investigation -- beyond what is required by this chapter -- may be needed to permit application of appropriate sanctions for violation of regulations, criminal prosecution, or determination of effective remedies for discovered vulnerabilities. The inquiry required by this chapter may serve as a part of these investigations, but notification of originators shall riot be delayed pending completion of these additional investigations.

**10-108 Unauthorized Absences**

When an individual who has had access to classified information is absent without authorization, the head of the activity or security manager shall determined if there are indications of activities, behavior, or associations that could indicate classified information may be at risk. If so, the supporting counterintelligence organization shall be notified. The scope and depth of this inquiry will depend on the length of the absence and the sensitivity of the classified information involved.