ENCLOSURE 6

SECURITY INCIDENTS INVOLVING CLASSIFIED INFORMATION

1. INTRODUCTION. Protection of classified information is essential to maintaining security and achieving mission success in DoD operational and warfighting environments. Prompt reporting of security incidents ensure that such incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of an actual loss or unauthorized disclosure of classified information and to preclude recurrence through an informed, properly tailored, and up-to-date security education and awareness program. In cases where compromise has been ruled out and there is no adverse effect on national security, a common sense approach to the early resolution of an incident at the lowest appropriate level is encouraged. All security incidents involving classified information shall involve a security inquiry, a security investigation, or both.

a. The terms associated with security incidents are formally defined in the Glossary, but to ensure common understanding, the following general characterizations are provided:

(1) Infraction. An infraction is a security incident involving failure to comply with requirements (i.e., the provisions of References (d) and (f), this Manual or other applicable security policy) which cannot reasonably be expected to, and does not, result in the loss, suspected compromise, or compromise of classified information. An infraction may be unintentional or inadvertent. While it does not constitute a security violation, if left uncorrected, can lead to security violations or compromises. It requires an inquiry to facilitate immediate corrective action but does not require an in-depth investigation.

(2) Violation. Violations are security incidents that indicate knowing, willful, and negligent for security regulations, and result in, or could be expected to result in, the loss or compromise of classified information. Security violations require an inquiry and/or investigation.

(a) Compromise. A compromise is a security incident (more specifically, a violation) in which there is an unauthorized disclosure of classified information (i.e., disclosure to a person(s) who does not have a valid clearance, authorized access, or a need to know).

(b) Loss. A loss occurs when classified information cannot be physically located or accounted for (e.g., classified information/equipment is discovered missing during an audit and cannot be immediately located).

(3) Inquiry. An inquiry is fact-finding and analysis conducted to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had, or could have had, access to the information. The inquiry identifies the facts, characterizes the incident as an infraction or a violation, identifies if possible the cause(s) and person(s) responsible, reports corrective actions taken or to be taken, and makes recommendations as to the need for further corrective action or a more in-depth investigation. Inquires, generally, are

initiated and conducted at the lowest echelon possible within the DoD Component.

(4) Investigation. An investigation is conducted for a security violation when the incident cannot be resolved via inquiry or for incidents where an in-depth and comprehensive examination of the matter is appropriate.

b. Certain practices dangerous to security, while not reportable as security incidents, have the potential to jeopardize the security of classified information and material if allowed to perpetuate. Examples of such practices are: placing a paper recycling box next to a classified copier or placing burn bags next to unclassified trash containers; stopping at a public establishment to conduct personal business while hand-carrying classified information; or failing to change security container combinations promptly when required. These practices, when identified, must be promptly addressed by security management and appropriate changes made, actions taken, or training provided, to ensure the security of classified information.

2. CONSEQUENCES OF COMPROMISE. The compromise of classified information presents a threat to the national security and may damage intelligence or operational capabilities; lessen the DoD ability to protect critical information, technologies, and programs; or reduce the effectiveness of DoD management. Once a compromise is known to have occurred, the seriousness of damage to U.S. national security or the extent of the adverse affect on the national security must be determined and appropriate measures taken to negate or minimize the adverse effects. When possible, action shall also be taken to regain custody of documents or material that was compromised. In all cases, security management must take appropriate action to identify the source and reason for the suspected or actual compromise and take remedial action to prevent recurrence.

3. REPORTING AND NOTIFICATIONS

a. Anyone finding classified information out of proper control shall, if possible, take custody of and safeguard the material and immediately notify the appropriate security authorities. Secure communications should be used for notification whenever possible.

b. Every civilian employee and Active, Reserve, and National Guard Military member of the Department of Defense, and every DoD contractor or employee of a contractor working with classified material, as provided by the terms of the contract, who becomes aware of the loss or potential compromise of classified information shall immediately report it to the head of his or her local activity and to the activity security manager.

c. If the person believes that the head of the activity or the security manager may have been involved in or responsible for the incident, he or she may report it to the security authorities at the next higher level of command or supervision. If circumstances of discovery make such notification impractical, the individual shall notify the commanding officer or security manager at the most readily available DoD facility or contact any DoD law enforcement, counterintelligence (CI), or Defense criminal investigative organization (DCIO).

d. Activity security officials shall advise their chain of command of compromises occurring within their area of security responsibility or involving assigned personnel.

e. 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 and, when appropriate, investigation are conducted, as needed, consistent with the requirements of this enclosure and corrective action is taken as required.

f. Reporting confirmed security incidents to the Director of Security, OUSD(I), is necessary when the incidents have or may have significant consequences or the fact of the incident may become public. Such incidents shall be reported promptly through appropriate security channels by the DoD Component senior agency official. When appropriate, preliminary reports shall be provided, particularly when the fact of the incident may become public or attract media attention.

(1) The Director of Security, OUSD(I), shall be notified of:

(a) A violation involving espionage.

(b) An unauthorized disclosure of classified information in the public media. See section 7 of this enclosure for information required in the notification. Additional notification is not required for reference to or republication of a previously identified media disclosure.

(c) Any violation wherein properly classified information is knowingly, willfully, or negligently disclosed to unauthorized persons or information is classified or continues to be classified when that violation:

1. Is reported to the oversight committees of Congress;

2. May attract significant public attention;

3. Involves large amounts of classified information; or

4. Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

(d) Any violation wherein a SAP is knowingly, willfully, or negligently created or continued contrary to the requirements of Reference (ah), DoDI O-5205.11 (Reference (bj)), this Manual, and national policies.

(e) A security failure or compromise of classified information relating to any defense operation, system, or technology that is likely to cause significant harm or damage to U.S. national security interests, for which Congressional reporting may be required by section 2723 of title 10, U.S.C. (Reference (bk)).

(f) Other egregious security incident (as determined by the DoD Component senior agency official).

(2) Security incidents that do not meet the reporting criteria specified above shall be filed in a retrievable format by the DoD Component and shall be available for inspection or further analysis, review, and potential investigation.

(3) On behalf of the Secretary of Defense, the USD(I) shall notify Congress and the Director, ISOO, regarding specific cases or incidents as required by References (d) and (bk).

(4) The Director of Security, OUSD(I), shall coordinate with the Office of the DNI (ODNI) National Counterintelligence Executive (NCIX) as needed to ensure notifications required by Intelligence Community Directive 701 (Reference (bl)) are made.

4. CLASSIFICATION OF REPORTS

a. Security incident reports shall be classified according to the content of the report and at the level prescribed by the applicable program security classification guides. At a minimum, reports shall be designated FOUO and marked as required by Volume 4 of this Manual, in order to provide appropriate protection for information regarding personnel involved and information that could facilitate unauthorized access to classified information. If the lost or compromised information is beyond the jurisdiction of the U.S. Government and cannot be recovered (e.g., media leak, public website posting, or loss in a foreign country), the report and location of the compromise (e.g., geographic location of unrecoverable equipment) shall be classified commensurate with the classification level of the compromised material to prevent further unauthorized disclosure.

b. If an FOUO report is to be disseminated outside the Department of Defense (e.g., to another Federal agency), the face of the document shall bear an expanded marking, as specified in Enclosure 3 of Volume 4 of this Manual, stating that the information may be exempt from mandatory disclosure pursuant to section 552 of title 5, U.S.C. (also known as "The Freedom of Information Act" and hereinafter referred to as "FOIA" (Reference (bm))).

c. Reports, whether classified or unclassified, disclosing technical data shall be marked with the appropriate distribution statement as described in DoDD 5230.24 (Reference (bn)) or associated with the information involved in the incident.

5. SPECIAL CIRCUMSTANCES. Certain types of classified information or specific circumstances require unique handling or consideration of additional reporting requirements as specified in paragraphs 5.a through 5.o.

a. Security Incidents Involving Deliberate Compromise, a Foreign Intelligence Service or a Terrorist Organization. Any incident in which deliberate compromise of classified information or involvement of a foreign intelligence service, international terrorist group, or organization is

suspected shall be reported immediately to the cognizant Defense CI component, in accordance with DoDD 5240.06 (Reference (bo)). Security officials shall not initiate or continue an inquiry or investigation of the incident unless it is fully coordinated with the cognizant Defense CI component.

b. Security Incidents Involving Apparent Violations of Criminal Law. Any incident in which an apparent violation of criminal law is suspected, but which is reasonably not believed to be espionage or involving matters described in paragraph 5.a of this section, shall be reported immediately to the local DCIO. If that organization accepts jurisdiction and initiates action, coordinate with them prior to taking any further action on the security inquiry or investigation so as not to jeopardize the integrity of either investigation.

c. Security Incidents Involving COMSEC or Cryptologic Information. Actual or potential compromises involving cryptographic information shall be handled according to NSTISSI 4003 (Reference (bp)).

d. Security Incidents Involving SCI. Actual or potential compromises involving SCI shall be reported to the activity SSO and handled in accordance with References (i) and (bl).

(1) Incidents involving SCI that meet the criteria in paragraph 3.f of this enclosure shall also be reported to the Director of Security, OUSD(I).

(2) If a DoD Component believes a disclosure may contain classified SCI information under the control of an(other) Intelligence Community agency, the DoD Component shall notify NCIX. NCIX shall coordinate notification to the affected agency.

e. Security Incidents Involving RD and/or FRD. In accordance with the provisions of section 3161 of Public Law 105-261 (Reference (bq)), and its implementing plan, the Secretary of Energy must report to Congress inadvertent disclosure of RD or FRD occurring pursuant to automatic declassification processes. Components shall notify the Department of Energy as necessary and provide a copy of the notification to the Deputy Assistant Secretary of Defense for Nuclear Matters and the Director of Security, OUSD(I).

f. Security Incidents Involving IT. Actual or potential compromises of classified information involving IT, automated information systems, or computer systems, terminals, or equipment shall be reported, in accordance with Reference (bf), through appropriate channels by the IA manager (IAM) to the activity security manager. Inquiries into and resolution of incidents involving compromise of classified information resident on computers or in IT systems require coordination with and assistance from the local IA officials, but prompt resolution remains the responsibility of the activity security manager. See Enclosure 7 for additional guidance on handling of classified data spills.

g. Security Incidents Involving FGI or NATO Information. Actual or potential compromises involving FGI or NATO information shall also be reported promptly by the DoD Component senior agency official to the USD(P), who serves as the DSA. The Director, International Security Programs, Defense Technology Security Administration, OUSD(P), shall be

responsible, on behalf of the DSA, for notifying and coordinating with NATO or the foreign government, as appropriate.

h. Security Incidents Involving Classified U.S. Information Provided to Foreign Governments. Actual or potential compromises of U.S. classified information held by foreign governments shall be reported to the originating DoD Component, the OCA, the Director of Security, OUSD(I), and the Director, International Security Programs, Defense Technology Security Administration, OUSD(P).

i. Security Incidents Involving SAPs. Actual or potential compromises involving DoD SAPs, or results of inquiries and/or investigations that indicate that weaknesses or vulnerabilities in established SAP policy and/or procedures contributed to an actual or potential compromise, shall be reported by the DoD Component SAP program office to the DoD SAP Central Office, which shall report to the Director of Security, OUSD(I).

j. Security Incidents Involving Improper Transfer of Classified Information. Any activity that receives classified information that has been improperly handled, addressed, packaged, transmitted, or transported shall make a determination as to whether the information has been subjected to compromise. If the activity determines that the classified information has been subjected to compromise, the receiving activity shall immediately notify the sending activity, which shall be responsible for initiating an inquiry or investigation, as appropriate. The receiving activity shall share information generated regarding the incident with the sending activity. The sending activity is responsible for required notifications (e.g., to the OCA). Classified information shall be considered as having been subjected to compromise if it has been handled through foreign postal systems, its shipping container has been damaged to an extent that the contents are exposed, or it has been transmitted (e.g., telephone, facsimile, message, e-mail, computer or data links) over communications circuits that are not approved for transmission of classified information. If the receiving activity determines that classified information was not in fact compromised, but was nevertheless improperly prepared or transferred, the receiving activity shall report the discrepancy to the sending activity.

k. Security Incidents Involving On-Site Contractors. Security incidents, including any inquiries or investigations required, involving on-site contractors shall be handled in accordance with paragraph C1.1.9 of Reference (ba). As specified by paragraph C1.1.9 of Reference (ba) and paragraph 6-105c of Reference (x), host activity security rules and procedures apply. Disciplinary action and sanctions are the responsibility of the contractor's company unless specific contract provisions address such actions. Security managers shall furnish the results of inquiries to the company, with a copy to Defense Security Service, in order to facilitate such action. Specified U.S. Government officials retain the ability, when appropriate and in accordance with the authorities and requirements of Reference (ba), to deny access to classified information, to revoke or suspend security clearances, and to take certain other administrative actions, such as to deny an individual continued access to the facility.

l. Security Incidents Involving Critical Program Information (CPI). Upon learning that classified CPI or CPI related to classified contracts may have been or was actually compromised, security officials shall inform the program manager of record and the cognizant Defense CI

component pursuant to DoDD O-5240.02 (Reference (br)). The specific CPI involved in the incident should be identified in inquiry and investigation reports. Classify reports as required by the applicable program security classification guide(s).

m. Security Incidents Involving ACCM-Protected Information. Security officials shall refer to section 18 of Enclosure 2 of this Volume for additional guidance on security incidents involving ACCM-protected information as well as safeguarding and handling of ACCM-protected information.

n. Absence Without Authorization. When an individual who has had access to classified information is absent without authorization, the head of the activity or security manager shall determine if there are indications of activities, behavior, or associations that could indicate classified information may be at risk. If so, the supporting Defense CI component shall be notified in accordance with Reference (br). The scope and depth of the inquiry shall depend on the length of absence and the sensitivity of the classified information involved. Missing personnel authorized SCI access shall be reported in accordance with Reference (i).

o. Coordination with Legal Counsel and the Department of Justice (DoJ). Whenever formal action, beyond adjudication of a finding of a security violation and assignment of reprimand or disciplinary action at the activity level is contemplated against any person believed responsible for the unauthorized disclosure of classified information, DoD Component officials shall coordinate with servicing legal counsel. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, Component officials shall use established procedures and channels to ensure coordination with the legal counsel of the DoD Component or Federal agency where the individual is assigned or employed and the DoJ.

6. SECURITY INQUIRIES AND INVESTIGATIONS

a. Requirement. All known or suspected instances of unauthorized disclosure of classified information shall be promptly addressed by the cognizant DoD Component to decide the nature and circumstances of the disclosure and the extent of damage to national security, and appropriate corrective action shall be taken. See Appendix 1 to this enclosure for a sample, optional format for use in documenting actions. Reports of inquiries and investigations, at a minimum, shall be designated and marked as FOUO.

b. Coordination with Criminal Investigative Organization or Defense CI Component. When information suggestive of a criminal or CI nature is discovered, all actions associated with the inquiry or investigation shall cease pending coordination with the cognizant DCIO or Defense CI component. If the DCIO or Defense CI component accepts jurisdiction, the inquiry or investigation shall not be resumed without agreement of the cognizant criminal investigative organization or CI component. All relevant information shall be released with an annotation in the report that the matter was referred to the specific DCIO or Defense CI component. Notify the OCA, originator, and others as appropriate, after coordination with the DCIO or Defense CI component. If the DCIO or Defense CI component declines jurisdiction, the security inquiry or investigation shall continue. Annotate the report appropriately and include the identity of the

official who made the declination decision and his or her organization.

c. Coordination with OCA

(1) If the inquiry or investigation determines that a compromise occurred, the official initiating the inquiry or investigation shall immediately notify the originator (i.e., the OCA) of the information or material involved. The OCA(s) shall take the actions required by section 9 of this enclosure.

(2) 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 or investigation or resolution of other related issues.

d. Security Inquiries. The head of the activity or activity security manager having security cognizance shall initiate an inquiry into the actual or potential compromise promptly to determine the facts and circumstances of the incident, and to characterize the incident as an infraction or a violation. At conclusion of the inquiry, a narrative of findings is provided in support of recommended additional investigative or other actions by the activity.

(1) The official appointed to lead the inquiry shall not be anyone involved with the incident. Preferably, the security manager should not be appointed to lead the inquiry.

(2) An inquiry shall be initiated and completed as soon as possible, not to exceed 10 duty days, and a report of findings provided to the activity head, activity security manager, and others as appropriate. If the inquiry cannot be completed within 10 duty days an extension should be requested from the appointing official.

(3) No recommendation should be made by an inquiry officer with regard to punitive action against the individual(s) responsible for the violation. An inquiry officer's function is to determine and report facts and make recommendations for actions needed to prevent future violations of the type investigated. Disciplinary or punitive action is the responsibility of the appropriate military commander or management official.

(4) If information obtained as a result of the inquiry is sufficient to provide answers to the following questions, then such information shall be sufficient to resolve the incident, to include instituting administrative sanctions consistent with section 17, Enclosure 3 of Volume 1 of this Manual.

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

(b) Was classified information compromised?

(c) If a compromise occurred, what specific classified information and/or material was involved? What is the classification level of the information disclosed?

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

(e) Was the information properly classified?

(f) Was the information officially released?

(g) In cases of compromise involving the public media:

1. In what specific media article, program, book, Internet posting or other item did the classified information appear?

2. To what extent was the compromised information disseminated or circulated?

3. Would further inquiry increase the damage caused by the compromise?

(h) Are there any leads to be investigated that might lead to identifying the person(s) responsible for the compromise?

(i) If there was no compromise, and if the incident was unintentional or inadvertent, was there a specific 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?

e. Security Investigations. If the circumstances of an incident require a more detailed or additional investigation, then an individual shall be appointed by the activity head in writing, to conduct that investigation and, as appropriate, provide recommendations for any corrective or disciplinary actions.

(1) The individual appointed shall be sufficiently senior to ensure a successful completion of the investigation and should be commensurate with the seriousness of the incident; have an appropriate security clearance; have the ability to conduct an effective investigation; and shall be someone unlikely to have been involved, directly or indirectly, in the incident.

(2) Except in unusual circumstances, the activity security manager shall not be appointed to conduct the investigation.

(3) As an investigation may lead to administrative or disciplinary action, the evidence developed should be comprehensive in nature and gathered in such a manner that it would be admissible in a legal or administrative proceeding. Consult local legal counsel as needed for procedural guidance on conduct of the investigation.

(4) The investigation should be accomplished promptly following appointment of the investigating officer. The results of the investigation shall be documented in writing. The format in Appendix 1 to this enclosure may be used.

7. INFORMATION APPEARING IN THE PUBLIC MEDIA

a. If classified information appears in the public media, including on public Internet sites, or if approached by a representative of the media, DoD personnel shall be careful not to make any statement or comment that confirms the accuracy of or verifies the information requiring protection. Report the matter as instructed by the appropriate DoD Component guidance, but do not discuss it with anyone who does not, in the case of classified information, have an appropriate security clearance and need to know.

b. If the fact of an unauthorized public disclosure becomes widely know, the Component senior agency official should consider whether the workforce needs to be reminded of actions to be or not to be taken by individuals in response to the disclosure. Reminders may include such topics as not viewing or downloading the classified information from unclassified IT systems, not confirming the accuracy of the information, and providing a point of contact for media inquiries.

c. Notifications of unauthorized disclosures of classified information in the public media required by subparagraph 3.f.(1)(b) of this enclosure shall include the information specified in subparagraphs 7.c.(1) through 7.c.(7). Initial notifications providing basic information about the incident and a point of contact should be made as quickly as is feasible; complete information should be provided subsequently.

(1) Date, location, and author of the public media item.

(2) Specific information disclosed and its classification level.

(3) Identification of the OCA.

(4) The extent to which the disclosed information was circulated, both within and outside the Department of Defense, and the number of persons known to have had access to the information.

(5) An appraisal of or statement regarding the damage to national defense and/or national security programs caused by the disclosure.

(6) A statement of whether any investigative leads exist and what additional actions, if any, are contemplated (i.e., no further action; administrative investigation by the DoD Component; referral to the cognizant DCIO for criminal investigation; or a request for USD(I) referral to DoJ for investigation).

(7) Point of contact for further information.

d. When notified of a suspected compromise of classified information through the public media, the USD(I) shall, unless already done by the reporting DoD Component, consult with the Assistant Secretary of Defense for Public Affairs and other officials having a primary interest in the information to determine if the information was officially released under proper authority.

e. When responsibility for an inquiry into an unauthorized public media disclosure is unclear or is shared equally with another DoD Component, refer the matter through security channels to the USD(I) who shall decide investigative responsibility in consultation with the affected DoD Components.

f. The decision on whether to initiate an additional investigation by a DCIO or by the Federal Bureau of Investigation through a referral to the DoJ shall be based on the following factors:

(1) The accuracy of the information disclosed.

(2) The damage to national security caused by the disclosure and whether there were compromises regarding sensitive aspects of current classified projects, intelligence sources, or intelligence methods.

(3) The extent to which the disclosed information was circulated, both within and outside the Department of Defense, and the number of persons known to have access to it.

(4) The degree to which an investigation shall increase the damage caused by the disclosure.

(5) The existence of any investigative leads.

(6) The reasonable expectation of repeated disclosures.

g. If the DoD Component's initial inquiry or investigation or a DCIO investigation identifies the person(s) responsible for an unauthorized disclosure of classified information via the public media or Internet, the DoD Component shall notify the Director of Security, OUSD(I). This notification shall include responses to the DoJ Media Leak Questionnaire (see Appendix 2 of this enclosure). The USD(I), in coordination with the General Counsel of the Department of Defense (GC, DoD) and the Head of the DoD Component having OCA, shall decide whether additional investigation is appropriate and whether to refer the unauthorized disclosure to the DoJ for investigation and/or criminal prosecution. When the initial inquiry or investigation does not identify the person responsible, the Head of the DoD Component, in consultation with the USD(I) and the GC, DoD, shall decide if further investigation is appropriate.

8. RESULTS OF INQUIRIES AND INVESTIGATIONS

a. If the conclusion of the inquiry or investigation is that a compromise occurred and that 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 due 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. Results of inquiries and/or investigations into actual or potential compromises that indicate that defects in the procedures and requirements of this Manual contributed to the incident shall be reported to the Director of Security, OUSD(I).

b. If the conclusion of the inquiry or 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 responsibility over such persons shall be responsible for taking action as may be appropriate to resolve the incident.

c. Additional investigation, beyond what is required by this enclosure, 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 this enclosure requires may serve as part of these investigations, but notifying OCAs shall not be delayed pending completion of these additional investigations.

9. ACTIONS TO BE TAKEN BY THE OCA. When notified of the compromise of classified information, the OCA shall:

a. Verify the classification and duration of classification initially assigned to the information.

b. Reevaluate the classification assigned to determine whether the classification shall be continued or changed. This classification review shall consider the following possibilities:

(1) 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.)

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

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

c. Advise the activity reporting the compromise of the outcome of the classification assessment required by paragraphs 9.a and 9.b of this section within 72 hours of notification.

d. Assess the impact of the compromise on the affected system, plan, program, or project; consider countermeasures (e.g., damage control actions) that may be taken to minimize, mitigate or limit damage to national security and prevent further loss or compromise; and then initiate or recommend adoption of such countermeasures.

(1) Where appropriate, countermeasures should be applied as quickly as possible and may be initiated prior to completion of the classification review or damage assessment.

(2) Countermeasures could include changing plans or system design features, revising operating procedures, providing increased protection to related information (e.g., classification upgrading), or other appropriate actions.

(3) Evaluate the cost implications of information, operational, or technology losses; developmental and integration costs of countermeasures; likelihood of countermeasure success; and programmatic impacts of the unmitigated loss and/or compromise of specific classified information.

e. Conduct a damage assessment as required by section 10 of this enclosure to determine the effect of the compromise of classified information on the national security.

10. DAMAGE ASSESSMENTS

a. A damage assessment is undertaken to determine the effect of a compromise on the national security.

(1) A damage assessment shall normally consist of a detailed, multidisciplinary examination of the facts surrounding the compromise to determine the practical effects of a compromise on DoD programs, operations, systems, materials, and intelligence and on the Department of Defense's ability to conduct its missions; to address mitigations and countermeasures that could be put in place to decrease or offset the impact; to determine the estimated dollar costs to implement countermeasures essential to maintain or reinstate security, or to replace weapons systems or capabilities that are thoroughly compromised; and to provide, when appropriate, specific recommendations for action.

(2) A damage assessment is conducted after the classification review and often follows any prosecutorial actions. However, when necessary to identify damage done by the disclosure or otherwise appropriate, a damage assessment may be conducted pre-prosecution.

(3) The damage assessment is not to be confused either with the classification review performed by the OCA or with damage control actions, which are those actions performed immediately upon the discovery of disclosure or compromise to minimize risk, limit damage, and/or prevent further loss or compromise.

b. Each DoD Component shall establish a system of controls and internal procedures to ensure that damage assessments are conducted, at a minimum, for cases of compromise involving espionage, intelligence information or compromise via the public media. Damage assessments are encouraged for other compromises.

(1) Conduct of the damage assessment is the responsibility of the OCA and subject

matter experts. Security officials should provide assistance as needed and appropriate.

(2) The results of relevant security inquiries and investigations shall be made available to inform the damage assessment process, as needed. Reports of criminal or CI investigations associated with the compromise should be requested by the OCA from the cognizant DCIO or Defense CI component.

11. VERIFICATION, REEVALUATION, AND DAMAGE ASSESSMENT TIMELINES. The verification and reevaluation steps in section 9 of this enclosure, and when appropriate the damage assessment process in section 10 of this enclosure, shall be completed as soon as possible following notification of a compromise. However, damage assessments requiring multi-disciplinary or multiple agency review of the adverse effects of the compromise on systems, operations, and/or intelligence, may sometimes be a long-term process. The DoD goal for completion of a damage assessment involving compromised classified information is no longer than 6 months from the first date the compromise was declared. Accomplishment of the assessment prior to the initiation of legal or administrative proceedings may be beneficial; check with legal counsel.

12. ACTUAL OR POTENTIAL COMPROMISES INVOLVING MORE THAN ONE AGENCY. When classified information under the control of more than one DoD Component or another Federal agency is involved, the affected activities are responsible for coordinating their efforts in evaluating the classification of information involved and assessing damage.

13. DEBRIEFING IN CASES OF UNAUTHORIZED ACCESS. In cases where unauthorized access to classified information has occurred, it may be advisable to discuss the situation with the individual(s) to enhance the probability that he or she shall properly protect it. The activity head shall determine if a debriefing is warranted. This decision shall be based on the circumstances of the incident, what is known about the person(s) involved, and the nature of the 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 U.S. Government contractor, who does not have a security clearance, debriefing is usually appropriate. The person shall be advised of his or her responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties that might follow if he or she fails to do so. The debriefing shall be designed to ensure that the individual understands the nature of the information, why its protection is important, and knows what to do if someone tries to obtain the information. In the case of non-DoD U.S. Government personnel and employees of U.S. Government contractors, the appropriate security official in the

individual's parent organization, including the appropriate facility security officer where applicable, shall be advised of the debriefing.

c. If the person involved is neither a member of a U.S. Government organization nor an employee of a U.S. Government contractor, the decision is much more situational. The key question is whether the debriefing shall have a 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, or to execute a SF 312. If an NDA is not executed, the nature and format of the statement is left to the discretion of the local security official to allow flexibility in meeting the requirements of a particular incident. If the person refuses to sign an NDA or debriefing statement when asked, this fact and his or her stated reasons for refusing shall be made a matter of record in the inquiry.

14. REPORTING AND OVERSIGHT MECHANISMS. The DoD Components shall establish necessary reporting and oversight mechanisms to ensure that inquiries and/or investigations are conducted when required, that they are done in a timely and efficient manner, and that appropriate management action is taken to correct identified problems. Inquiries or investigations and management analyses of security incidents shall 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., shall be considered in determining causes and contributing factors. The focus of management response to security incidents shall be to eliminate or minimize the probability of further incidents occurring. Appropriate disciplinary action or legal prosecution, as discussed in section 17, Enclosure 3 of Volume 1 of this Manual, is sometimes one means of doing this, but the broader focus on prevention shall not be lost. Simple disciplinary action, without consideration of what other factors may have contributed to the situation, shall not be considered an acceptable response to a security incident.

Appendixes
1. Security Incident Reporting Format
2. DOJ Media Leak Questionnaire

APPENDIX 1 TO ENCLOSURE 6

SECURITY INCIDENT REPORTING FORMAT

1. The report format as described in Figure 2 is optional, to be used as a guide for appropriate content. The format may be used as shown or tailored to suit the organization and the circumstances. In all cases, the goal is to identify who, what, when, where, why, and how the incident occurred and to determine what should be done to preclude similar incidents in the future.

2. Classify, and appropriately mark, security incident reports according to content. At a minimum, reports shall be designated and marked "FOR OFFICIAL USE ONLY" as the reports will contain information on personnel involved. The reports may also contain other information that qualifies for designation as FOUO and information that could facilitate unauthorized access to classified information.

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, weak, out-of-date, unenforceable, ineffective, etc.). Include any assessment regarding systemic weaknesses or vulnerabilities in established security practices (e.g., non-existent, out-of-date, or ineffective policies, procedures or training) that must be corrected; suggest the corrective actions required.

3. Actions taken: List actions that have been taken (e.g., notifications made, messages sent, interviews with, counseling of, and discipline rendered for individuals involved, and other information as required). Include dates inquiry or investigation started and ended.

4. Recommendations: Make recommendations concerning what should be done to preclude future incidents of this type.

5. Identification of inquiry or investigating official, organization, and telephone numbers.

6. Evaluation notes. Enter other information relevant to the inquiry or investigation. Attach interview statements and/or records, documentary evidence, exhibits and so forth, as appropriate.

(Signature of Inquiry or Investigating Official)

FOR OFFICIAL USE ONLY (or, if classified, insert classification and add other markings as required)

APPENDIX 2 TO ENCLOSURE 6

DOJ MEDIA LEAK QUESTIONNAIRE

If the initial inquiry and/or investigation into an unauthorized disclosure of classified information via the media identifies the person responsible for the unauthorized disclosure, the Head of the DoD Component shall promptly answer to the fullest extent possible the standard questions in this appendix, which comprise the DoJ Media Leak Questionnaire, and submit the questionnaire through security channels to the USD(I). In coordination with the GC, DoD, the USD(I) shall, when warranted, forward the information via letter to:

Department of Justice, Criminal Division
Attention: Chief, Internal Security Section
Bond Building, Room 9400
1400 New York Avenue, NW
Washington, DC 20530

a. What is the date and identity of the media source (e.g., article, blog, television, or other oral presentation) containing classified information?

b. What specific statement(s) in the media source are classified and was the information properly classified?

c. Is the classified information disclosed accurate?

d. Did the information come from a specific document, and if so, what is the origin of the document and the name of the individual responsible for the security of the classified data discussed?

e. What is the extent of official circulation of the information?

f. Has the information been the subject of prior official release?

g. Was prior clearance for publication or release of the information sought from proper authorities?

h. Has the material, parts thereof or enough background data, been published officially or in the press to make an educated speculation on the matter possible?

i. Will the information be made available for use in a prosecution, and if so, what is the name of the person competent to testify on its classification?

j. Was declassification considered or decided on before the data appeared in the media?

k. What effect might the disclosure of the classified data have on the national defense?