Job Aid

Special Circumstances for Reporting Security Incidents

Certain types of classified information or specific circumstances require unique handling or consideration of additional reporting requirements.

Information	Processing Requirement(s)
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. 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.
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 a deliberate compromise involving a Foreign Intelligence Service or a terrorist organization, 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.
COMSEC or Cryptologic Information	Actual or potential compromises involving cryptographic information shall be handled according to NSTISSI 4003.
Sensitive Compartmented Information	Actual or potential compromises involving SCI shall be reported to the activity SSO and handled in accordance with DoD 5105.21-M-1, "Department of Defense Sensitive Compartmented Information Administrative Security Manual," October 2012 and Intelligence Community Directive 701, "Security Policy Directive for Unauthorized Disclosures of Classified Information," March 14, 2007. 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

Information	Processing Requirement(s)
	notify NCIX. NCIX shall coordinate notification to the affected agency.
Restricted Data (RD) and/or Formerly Restricted Data (FRD)	In accordance with the provisions of section 3161 of Public Law 105-26, 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).
Information Technology	Actual or potential compromises of classified information involving IT, automated information systems, or computer systems, terminals, or equipment shall be reported, in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, 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 DoDM 5200.01, Volume 3, Enclosure 7 for additional guidance on handling of classified data spills.
Foreign Government Information (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.
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)

Information	Processing Requirement(s)
Special Access Programs (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).
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.

Information	Processing Requirement(s)
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 DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985. As specified by this reference and paragraph 6-105c of DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, 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 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.
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. 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).
Alternative Compensatory Control Measures (ACCM)-Protected Information	Security officials shall refer to DoDM 5200.01, Volume 3, Enclosure 2, section 18 for additional guidance on security incidents involving ACCM-protected information as well as safeguarding and handling of ACCM-protected information.
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 DoD Directive O-5240.02, "Counterintelligence," December 20, 2007. 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 DoD 5105.21-M-1, "Department of Defense Sensitive Compartmented Information Administrative Security Manual," October 2012.

Information	Processing Requirement(s)
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.