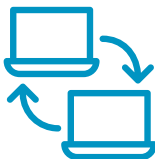








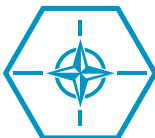


Job Aid: Special Types of Security Incidents




Introduction: The following table explains special types of security incidents and specific actions that should be taken when they occur. For these incidents, the Activity Security Manager (ASM) must determine other officials who should be notified based on the information involved in an actual or potential compromise.

Type of Security Incident	Action
<p>Improper transfer of classified information and spillage</p> 	<ul style="list-style-type: none">• Coordinate with the sending activity to notify the Original Classification Authority (OCA).• Determine if the person has put classified information at risk and contact the cognizant authority.• Reference for spillage actions:<ul style="list-style-type: none">○ DODM 5200.01, Volume 3, DOD Information Security Program, Protection of Classified Information, Enclosure 7○ The Committee on National Security Systems (CNSS) Policy 18, National Policy on Classified Information Spillage, for the framework on addressing national security information spillage○ CNSS Instruction 1001 for questions to ask when investigating spillage
<p>Apparent violations of criminal law</p> 	<p>Notify Defense Criminal Investigative Organization (DCIO) for violations of criminal law where espionage is not suspected.</p>
<p>Communications Security (COMSEC) or Cryptologic</p> 	<p>Actual or potential compromises involving cryptographic information shall be handled according to the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4003, Reporting and Evaluating COMSEC Incidents.</p>



Type of Security Incident	Action
<p>Sensitive Compartmented Information (SCI)</p> 	<ul style="list-style-type: none">• Report to the activity Special Security Officer (SSO), Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) for incidents involving SCI that meet the criteria found in DODM 5200.01, Vol. 3, DOD Information Security Program, Protection of Classified Information, Enclosure 7.• Notify Office of the National Counterintelligence Executive (NCIX) if another intelligence community agency is involved.
<p>Restricted Data (RD)/Formerly Restricted Data (FRD)</p> 	<p>Notify the Department of Energy (DOE) as necessary and provide a copy of the notification to the Deputy Assistant Secretary of Defense for Nuclear Matters and the Director of Security, Office of the OUSD(I&S).</p>
<p>Information Technology (IT)</p> 	<p>Report to appropriate channels via the Information Assurance Manager (IAM)/Information Systems Security Manger (ISSM) to the ASM:</p> <ul style="list-style-type: none">• Coordinate with IA officials, as necessary.• Reference DODI 8500.01, "Cybersecurity,"• Also reference <i>Improper Transfer of Classified Information</i> in this job aid.
<p>Deliberate Compromise, Foreign Intelligence Service or Terrorist Organization</p> 	<p>Notify the cognizant Defense Counterintelligence (CI) Component in accordance with DODD 5240.06, "Counterintelligence Awareness and Reporting (CIAR)."</p>
<p>Foreign Government Information (FGI) or North Atlantic Treaty Organization (NATO) Information</p> 	<p>Incidents involving FGI or NATO Information:</p> <ul style="list-style-type: none">• DOD components should promptly report to the Designated Security Authority (DSA)• The Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy (OUSD(P)), is responsible, on behalf of the DSA for notifying NATO or the Foreign government of incident



Type of Security Incident	Action
	Incidents involving compromise of US classified held by foreign governments: <ul style="list-style-type: none">Report to originating DOD component, OCA, the Director of Security, OUSD(I&S), and the Director, International Security Programs, Defense Technology Security Administration, OUSD(P).
Special Access Programs (SAP) 	Shall be reported by the DOD Component SAP program office to the DOD SAP Central Office, which will report the incident to the Director of Security, OUSD(I&S).
Critical Program Information (CPI) 	<ul style="list-style-type: none">Security officials shall inform the program manager and the cognizant Defense CI component in accordance with DODD 5240.02, "Counterintelligence."The specific CPI involved should be identified.
Alternative Compensatory Control Measures (ACCM) 	<ul style="list-style-type: none">Immediately notify the ACCM control officer, or security manager.Reporting, inquiry and investigation, and additional measures should occur in accordance with DODM 5200.01, Volume 3, DOD Information Security Program, Protection of Classified Information, Enclosure 2.