



CDSE
Center for Development
of Security Excellence

INDUSTRIAL SECURITY JOB AID



This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE FSO Toolkit).

Reporting Topic	What to Report	How to Report	Report Recipient
Espionage Sabotage Terrorism Subversive Activities	Any known information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any of the contractor's sites	<p>In writing. If the matter is urgent, the initial report may be made by phone and must be followed up in writing (i.e., email, formal correspondence)</p> <p>When a report is made to the Federal Bureau of Investigation (FBI), promptly notify your Industrial Security Representative (IS Rep) at the DCSA Field Office and provide a copy of the written report</p>	<p>FBI</p> <p>Notify and provide copy of written report to IS Rep</p>
Adverse Information	<p>Any information that negatively reflects on the integrity or character of a cleared employee that suggests his or her ability to safeguard classified information may be impaired, that his or her access to classified information may not be in the interest of national security, or that the individual constitutes an insider threat. Reporting should be based on references in SEAD 4, National Security Adjudicative Guidelines. Some examples include:</p> <ul style="list-style-type: none">• Allegiance to the United States• Foreign influence/preference• Personal conduct• Financial considerations• Drug involvement/substance misuse• Criminal conduct• Use of information technology <p><i>Do not report information based on rumor or innuendo.</i></p>	Appropriate function in the DoD Personnel Security System of Record (i.e., Incident Report in Defense Information System for Security (DISS))	Vetting Risk Operations Center (VROC)



CDSE
Center for Development
of Security Excellence

INDUSTRIAL SECURITY JOB AID



This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE FSO Toolkit).

Reporting Topic	What to Report	How to Report	Report Recipient
Suspicious Contacts	<ul style="list-style-type: none"> • Efforts by any individual, regardless of nationality, to gain illegal or unauthorized access to classified information • Efforts by any individual, regardless of nationality, to elicit information from an employee determined eligible for access to classified information, and any contact that suggests the employee may be the target of an attempted exploitation by an intelligence service of another country • All contacts by employees determined eligible for access to classified information with known or suspected intelligence officers from any country 	In writing	IS Rep and Counterintelligence Special Agent (CISA)
Change in Status of Employee Determined Eligible for Access to Classified Information	<p>The following changes in the personal status include:</p> <ul style="list-style-type: none"> • Death • Change in name • Termination of employment • Change in citizenship 	Enter changes as applicable in the DoD Personnel Security System of Record (i.e., DISS)	VROC
Citizenship by Naturalization	<p>If a non-U.S citizen employee granted a Limited Access Authorization (LAA) becomes a citizen through naturalization. The report will include:</p> <ul style="list-style-type: none"> • City, county, and state where naturalized • Date naturalized • Court • Certificate number 	Appropriate function in the DoD Personnel Security System of Record (i.e. Customer Service Request (CSR) in DISS)	VROC
Employees Desiring Not To Be Processed For A National Security Eligibility Determination or Not To Perform Classified Work	<ul style="list-style-type: none"> • Any employee who no longer wishes to be processed for a determination of eligibility for access to classified information • Any employee who no longer wishes to continue having access to classified information. 	Enter the reason in the appropriate function in the DoD Personnel Security System of Record (i.e. Customer Service Request (CSR) in DISS)	VROC



CDSE
Center for Development
of Security Excellence

INDUSTRIAL SECURITY JOB AID



This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE FSO Toolkit).

Reporting Topic	What to Report	How to Report	Report Recipient
Classified Information Nondisclosure Agreement (NDA)	The refusal by an employee to sign the SF-312, Classified Information Nondisclosure Agreement, or other approved NDA	Enter the reason in the appropriate function in the DoD Personnel Security System of Record (i.e. Customer Service Request (CSR) in DISS)	VROC
Changed Conditions Affecting the Contractor's Eligibility for Access to Classified Information (e.g., Facility Clearance (FCL))	<ul style="list-style-type: none"> • Change of ownership or control • Change of operating name or address • Change to information previously submitted for Key Management Personnel (KMP) • Any action to terminate business or operations • Any material change concerning information previously reported concerning Foreign Ownership, Control, or Influence (FOCI) <ul style="list-style-type: none"> ○ Submit a revised Certificate Pertaining to Foreign Interests (SF-328) ○ Submit a copy of Schedule 13D, if received 	FCL System of Record (i.e., National Industrial Security System (NISS))	IS Rep (via NISS)
Changes in Storage Capability	Any change in the facility's storage requirement or capability to safeguard classified material	In writing	IS Rep
Inability to Safeguard Classified Material	Any emergency situation that renders the facility (or their location) incapable of safeguarding classified material	In writing	IS Rep
Security Equipment Vulnerabilities	Significant vulnerabilities identified in security equipment, such as: <ul style="list-style-type: none"> • Intrusion Detection Systems (IDS) • Access control systems • Communications Security (COMSEC) equipment or systems • Information System (IS) security hardware and software 	In writing	IS Rep



CDSE
Center for Development
of Security Excellence

INDUSTRIAL SECURITY JOB AID



This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE FSO Toolkit).

Reporting Topic	What to Report	How to Report	Report Recipient
Unauthorized Receipt of Classified Material	The receipt or discovery of any classified material that the contractor is not authorized to have. Report should identify: <ul style="list-style-type: none">• Source (sender)• Originator (generated material)• Quantity (pages, volumes)• Subject or title• Date material was generated• Classification level (markings)	In writing	IS Rep
Employee Information in Compromise Cases	Report upon request of Cognizant Security Agency (CSA) only; information concerning an employee in connection with the loss, compromise, or suspected compromise of classified information	In writing	IS Rep
Disposition of Classified Material Terminated From Accountability	The whereabouts or disposition of material terminated from accountability is subsequently discovered and brought back into accountability	In writing	IS Rep
Foreign Classified Contracts	Any pre-contract negotiation or award not placed through the CSA or U.S. Government Contracting Activity (GCA) that involves or may involve: <ul style="list-style-type: none">• The release or disclosure of U.S. classified information to a foreign interest• Access to classified information furnished by a foreign interest	In writing	IS Rep



CDSE
Center for Development
of Security Excellence

INDUSTRIAL SECURITY JOB AID



This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located in the CDSE FSO Toolkit).

Reporting Topic	What to Report	How to Report	Report Recipient
Loss, Compromise, or Suspected Compromise	<p>The loss, compromise, or suspected compromise of classified information, U.S. or foreign</p> <p>If the preliminary inquiry finds no compromise, then the completed inquiry should be filed until examined by your IS Rep on the next facility security review.</p>	In writing (initial and final report)	IS Rep
Individual Culpability	<p>The determination of an individual's responsibility for a security violation can be determined when one or more of the following factors are evident:</p> <ul style="list-style-type: none">• Deliberate disregard of security requirements• Gross negligence in the handling of classified material• A pattern of questionable judgement, irresponsibility, negligence, or carelessness <p>Report should include:</p> <ul style="list-style-type: none">• Statement of the administrative actions against the employee• Details of the incident(s)	Appropriate function in the DoD Personnel Security System of Record (i.e., Incident Report in DISS)	VROC