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	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) When a report is made to the FBI, promptly notify your Industrial Security Representative (IS Rep) at the Defense Counterintelligence and Security Agency (DCSA) Field Office and provide a copy of the written report	FBI Notify and provide copy of written report to IS Rep
Adverse Information	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: • Allegiance to the United States • Foreign influence/preference • Personal conduct • Financial considerations • Drug involvement/substance misuse • Criminal conduct • Use of information technology *Do not report information based on rumor or innuendo.*	Appropriate function in the DOD Personnel Security System of Record (i.e., Incident Report in Defense Information System for Security (DISS))	Vetting Risk Operations (VRO)

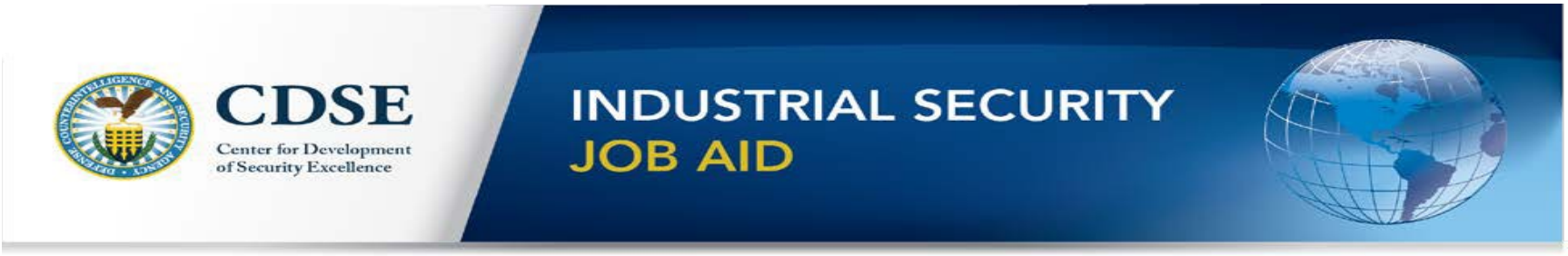
This job aid provides guidance to assist contractors with general examples for reporting. Please refer to the National Industrial Security Program Operating Manual (NISPOM) and the Security Executive Agent Directive (SEAD) 3 for an entire list of reportable activities and reporting requirements (located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

Reporting Topic	What to Report	How to Report	Report Recipient
Change in Status of Employee Determined Eligible for Access to Classified Information	The following changes in the personal status include: • 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)	VRO
Citizenship by Naturalization	If a non-U.S. citizen employee granted a Limited Access Authorization (LAA) becomes a citizen through naturalization, the report will include: • 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)	VRO
Employees Desiring Not To Be Processed For A National Security Eligibility Determination or Not To Perform Classified Work	• 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. CSR in DISS)	VRO
Reporting Topic	**What to Report**	**How to Report**	**Report Recipient**
Refusal to sign Standard Form (SF) 312 Classified Information Nondisclosure Agreement (NDA)	An employee refuses 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. CSR in DISS)	VRO
Individual Culpability	The determination of an individual's responsibility for a security violation can be determined when one or more of the following factors are evident: • Deliberate disregard of security requirements • Negligence in the handling of classified material	Appropriate function in the DOD Personnel Security System of Record (i.e., Incident Report in DISS)	VRO

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).

	• A pattern of questionable judgement, irresponsibility, negligence, or carelessness Report should include: • Statement of the administrative actions against the employee • Details of the incident(s)		
Suspicious Contacts	• 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)

Changed Conditions Affecting the Contractor's Eligibility for Access to Classified Information (e.g., Facility Clearance (FCL))	• 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 as Foreign Ownership, Control, or Influence (FOCI)
	  ○ 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)



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).

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
Unsatisfactory Conditions of a Prime or Subcontractors	Any information that indicates classified information cannot be adequately protected by a prime or subcontractor, or other circumstances that may impact the eligibility for access to classified information by any prime or subcontractors	In writing	IS Rep
Reporting by subcontractor	Subcontractors will also notify their prime contractors if they make any reports to their Cognizant Security Agency (CSA)	In writing	IS Rep and Prime Contractor
Dispositioned Material Previously Terminated	When the location or disposition of classified material previously terminated from accountability is subsequently discovered and brought back into accountability	In writing	IS Rep
Reporting Topic	**What to Report**	**How to Report**	**Report Recipient**
Improper Receipt of Foreign Government Material	The receipt of classified information from foreign interests that is not received through U.S. Government channels. Report should identify: • 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 CSA only; information concerning an employee in connection with the loss, compromise, or suspected compromise of classified information	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:	In writing	IS Rep

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).

	• The release or disclosure of U.S. classified information to a foreign interest • Access to classified information furnished by a foreign interest		
Reporting Topic	**What to Report**	**How to Report**	**Report Recipient**
Loss, Compromise, or Suspected Compromise	The loss, compromise, or suspected compromise of classified information, U.S. or foreign If the preliminary inquiry finds no compromise, then the completed inquiry should be filed until it can be examined by your IS Rep on the next facility security review	In writing (initial and final report)	IS Rep
Cyber Incident Reports	Any cyber incident on a classified covered information system that has been approved by that CSA to process classified information	In writing	IS Rep
Reporting Topic	**What to Report**	**How to Report**	**Report Recipient**
Foreign Travel (UNOFFICIAL)	Prior approval of unofficial foreign travel is required to be reported. • The cleared employee notifies the cleared contractor (e.g., FSO or assigned designee) before foreign travel. If notification does not occur in advance, the covered individual must notify the cleared contractor as soon as possible after the travel occurs, not to exceed five business days • The cleared employee submits a complete travel itinerary to the cleared contractor. And, the cleared contractor reports the travel prior to the unofficial foreign travel • The cleared contractor provides the covered individual with the National Counterintelligence and Security Center (NCSC) “Safe Travels” resource • The cleared contractor coordinates with a DCSA CISA	Appropriate function in the DOD Personnel Security System of Record (i.e., Foreign Travel in DISS) and if applicable, in writing	VRO and if applicable, CISA

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).

	for appropriate pre-foreign travel briefings when the covered individual is traveling to a foreign country listed in the Director of National Intelligence's Worldwide Threat Assessment of the U.S. Intelligence Community		
Foreign Contacts (UNOFFICIAL)	Any contact with a foreign national involving the exchange of personal information A reportable instance involving an exchange of personal information with a foreign national would meet the following criteria: • The name and nationality of the foreign national are known by the cleared individual during or after the exchange of personal information, and • The nature of the personal information provided by the cleared individual to the foreign national is not reasonably expected to be accessible by the general public, nor to be willingly released to the general public by the cleared individual, and • Contact with the foreign national is re-occurring or expected to re-occur	Appropriate function in the DOD Personnel Security System of Record (i.e., CSR in DISS)	VRO