DEPARTMENT OF DEFENSE
DEFENSE SECURITY SERVICE
27130 Telegraph Road, Quantico, VA 22134

INDUSTRIAL SECURITY LETTER

Industrial Security Letters (ISLs) are issued periodically to inform cleared contractors, government contracting activities and DoD activities of developments relating to industrial security. These letters are for information and clarification of existing policy and requirements. Suggestions for ISLs are appreciated and should be submitted to the local Defense Security Service Industrial Security Field Office. Please address specific inquiries about this ISL to DSS.

ISL 2016-02 **May 21, 2016**

(Revised June 29, 2017)

On May 18, 2016, the Department of Defense published Change 2 to DoD 5220.22-M, "National Industrial Security Manual Operating Manual (NISPOM)." NISPOM Change 2 requires contractors[1] to establish and maintain an insider threat program to detect, deter and mitigate insider threats. Specifically, the program must gather, integrate, and report relevant and credible information covered by any of the 13 personnel security adjudicative guidelines[2] that is indicative of a potential or actual insider threat to deter cleared employees[3] from becoming insider threats; detect insiders[4] who pose a risk to classified information; and mitigate the risk of an insider threat.[5] Contractors must have a written program plan in place to begin implementing insider threat requirements of Change 2 no later than November 30, 2016. This Industrial Security Letter (ISL) provides clarification and guidance to assist contractors as they establish and tailor an insider threat program to meet NISPOM Change 2 requirements. Nothing in this ISL alters or supersedes the text of the published NISPOM Change 2.

Insider Threat Minimum Standards for Contractors

NISPOM 1-202 requires the contractor to establish and maintain an insider threat program that will gather, integrate, and report relevant and available information indicative of a potential or actual insider threat. DSS will consider the size and complexity of the cleared facility in assessing its implementation of an insider threat program to comply with NISPOM Change 2.

---

[1] "Contractor" refers to any industrial, educational, commercial, or other entity that has been granted a facility security clearance (FCL) by a Cognizant Security Agency (CSA). (NISPOM Appendix C)

[2] http://www.gpo.gov/fdsys/pkg/CFR-2012-title32-vol1/xml/CFR-2012-title32-vol1-part147.xml

[3] All contractor employees granted personnel security clearances (PCLs) and all employees being processed for PCLs as defined by the NISPOM. (NISPOM Appendix C)

[4] Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems. (NISPOM Appendix C)

[5] Insider threat is defined as "the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information." (NISPOM Appendix C)

Contractor programs must include the following elements:

- **1-202a**. An insider threat program plan endorsed by the insider threat program senior official (ITPSO) describing:

    - Capability to gather relevant insider threat information across the contractor facility (e.g., human resources, security, information assurance, legal), commensurate with the organization's size and operations.

    - Procedures to access, share, compile, identify, collaborate among the cleared contractor's functional elements (including those listed above), and report relevant information covered by the 13 personnel security adjudicative guidelines that may be indicative of a potential or actual insider threat; to deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risk of an insider threat.

    - Any corporate-wide program plans that address requirements for all cleared facilities within the corporate family and address effective implementation at each cleared entity within the business structure.

Contractors will self-certify to DSS that a written program plan is implemented and current.

- **1-202b.** Formal appointment by the contractor of an ITPSO who is a U.S. citizen employee and a senior official of the company:

    - The ITPSO will be cleared in connection with the FCL and is responsible for establishing and executing the contractor's insider threat program.

    - The ITPSO must serve in a position within the organization that has the authority to provide management, accountability, and oversight to effectively implement and manage the requirements of the NISPOM related to insider threat.

    - The facility security officer (FSO) may also serve as the ITPSO. If the ITPSO is not the FSO, the contractor's ITPSO will ensure the FSO is an integral member of the contractor's implementation program for an insider threat program.

    - Contractors will appoint the ITPSO as one of the company's key management personnel in the Electronic Facility Clearance System (e-FCL) at http://www.dss.mil/is/efcl.html or as directed by the CSA. Additional information is available at www.dss.mil.

- **1-202c**. Appointment of an ITPSO for the corporate family:

    - A corporate family may choose to establish a corporate-wide insider threat program with one senior official appointed to establish and execute the program.

- Each cleared legal entity in the corporate family using the corporate-wide ITPSO must separately appoint that person as the ITPSO for that cleared legal entity in e-FCL at http://www.dss.mil/is/efcl.html.

- If the corporate family chooses to have the corporate-wide ITPSO also serve as the senior official for cleared divisions or branches within a multiple-facility organization, the ITPSO will provide DSS a list of facilities by Commercial and Government Entity (CAGE) code for which the ITPSO serves as the senior official. DSS, in its discretion, may also require that the ITPSO, if appointed for all the cleared facilities within a multiple-facility organization, be submitted in e-FCL at http://www.dss.mil/is/efcl.html for each cleared facility.

- When a corporate family appoints a single ITPSO, that individual must be able to effectively manage the insider threat requirements for each entity for which they are appointed or maintain a record of the individuals at each cleared facility who are trained in accordance with this ISL to support implementation of insider threat program requirements.

- **1-207b.** Contractor reviews:

  - A senior management official at the cleared facility will certify annually to DSS in writing that a self-inspection has been completed in accordance with the provisions of NISPOM paragraph 1-207b.

  - Contractors must make self-inspection reports available to DSS during the next security vulnerability assessment following the self-inspection.

  - Additional guidance is in the Self-Inspection Handbook for NISP Contractors at http://www.cdse.edu/documents/cdse/self_inspect_handbook_nisp.pdf. The Self-Inspection Handbook includes guidance on implementing insider threat program requirements.

- **1-300.** Reporting requirements:

  - This ISL does not change the reporting requirements of the NISPOM Change 2; it serves to clarify the reporting requirements related to behaviors indicative of insider threat.

  - Contractors must report relevant and credible information coming to their attention regarding cleared employees. Such reporting includes information indicative of a potential or actual insider threat that is covered by any of the 13 personnel security adjudicative guidelines http://www.gpo.gov/fdsys/pkg/CFR-2012-title32-vol1/xml/CFR-2012-title32-vol1-part147.xml, or when that information constitutes adverse information, in accordance with NISPOM 1-302a. (further clarified in "ISL 2011-04, "Adverse Information").

Training and information on the Federal adjudicative guidelines is available from the DSS Center for Development of Security Excellence (CDSE) at http://www.cdse.edu/shorts/personnel-security.html.

- **1-304**. Individual culpability reports: Contractors must have a system or process to identify patterns of negligence or carelessness in handling classified information to ensure reporting in accordance with the requirements outlined NISPOM 1-304c, even for incidents that do not initially warrant a culpability or individual incident report.

- **3-103.** Insider threat training:

  - **3-103.a.** Insider threat personnel assigned duties related to insider threat program management: Training on insider threat program management is required for all personnel assigned duties related to insider threat program management. Contractors must provide internal training for insider threat program personnel that includes, at a minimum, the topics outlined in NISPOM 3-103a. Contractors may use an existing training course to meet the training requirements for insider threat program personnel. CSA-designated training that meets the minimum topics outlined in NISPOM 3-103 is available through the CDSE catalog under Insider Threat at http://www.cdse.edu/catalog/insider-threat.html *See Establishing an Insider Threat Program for Your Organization, course INT122.16.*

    After initial implementation of NISPOM Change 2, new contractor personnel assigned duties related to insider threat program management must complete the required training within 30 days of being assigned those duties.

  - **3-103.b.** Employee awareness: Training on insider threat awareness is required for all cleared employees before being granted access to classified information and annually thereafter. Contractors must provide internal training programs that include, at a minimum, the topics outlined in NISPOM 3-103b. Contractors may use an existing training course to meet the requirements of insider threat awareness training for personnel who access classified information. Training is available through the CDSE catalog under Insider Threat. *See Insider Threat Awareness, course INT101.16, or Counterintelligence Awareness and Security Briefing, course CI112.16.* These courses are available at https://securityawareness.usalearning.gov/itawareness/index.htm and http://www.cdse.edu/catalog/elearning/CI112.html .

  - **3-103b.** Insider threat awareness training: All cleared employees who are not currently in access must complete insider threat awareness training prior to being granted access. Cleared employees already in access must complete insider threat awareness training within 12 months of the issuance date of NISPOM Change 2 (i.e., no later than May 17, 2017).

  - **3-103c.** Training records management: Contractors must create and maintain records of all employee insider threat awareness program initial and refresher training. Records of training must be available for review during DSS security vulnerability assessments and

must consist of training attendance certificates, or other documentation verifying that personnel required to complete the training requirements outlined in this ISL have completed the training.

- **3-108.** Refresher training: Contractors will include insider threat awareness in annual refresher training to reinforce and update cleared employees on the information provided in initial training.

- **8-100d.** User activity monitoring on classified information systems:

  - Contractors must implement the DSS-provided information system security controls on classified information systems in order to detect activity indicative of insider threat behavior. These controls are based on Federal requirements and standards (Federal Information Security Management Act, National Institute of Standards and Technology, and Committee for National Security Systems).

  - Additional guidance for information systems under DSS industrial security cognizance has been incorporated into the DSS Office of the Designated Approving Authority (ODAA) Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM, known as the ODAA Process Manual. The ODAA Process Manual is available at http://www.dss.mil/isp/odaa/odaa.html.

- **8-200. Overview.** The term "authorizing official" has replaced the term "designated approving authority" in the NISPOM. The DSS ODAA serves as the authorizing official to render an operational authorization decision for contractors based on the results of security assessment activities and the implementation of the set of security controls provided by DSS.

The CDSE Industry Insider Threat Job Aid provides additional information and guidance on these requirements at http://www.cdse.edu/catalog/insider-threat.html. Training, job aids and best practices are available in the Insider Threat Tool Kit at http://www.cdse.edu/toolkits/insider/index.php.