DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

INDUSTRIAL SECURITY LETTER

Industrial security letters (ISLs) are issued as necessary to inform cleared contractors, Government contracting activities, and DoD Components of developments relating to the National Industrial Security Program (NISP). The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or departmental policies.

ISL 2026-01 **Date: May 20, 2026**

In accordance with Title 32, Code of Federal Regulations (CFR), Part 117, the "National Industrial Security Program Operating Manual (NISPOM)," cleared contractors are directed to implement insider threat programs. This requirement, outlined in NISPOM 117.7(d), stems from Executive Order 13587 and the Presidential Memorandum on "National Insider Threat Policy and Minimum Standards."

This ISL provides a consolidated overview of minimum standards, resources, and training to assist contractors in establishing and tailoring their programs. The Defense Counterintelligence and Security Agency (DCSA) will assess program compliance, which must be included in the contractor's annual self-inspection.

Insider Threat Program: Minimum Standards

Requirement	Details
Insider Threat Plan	Contractors must create and maintain written procedures for their insider threat program to deter and detect potential threats in accordance with NISPOM 117.7(b)(4). The Center for Development of Security Excellence (CDSE) provides a sample plan for reference.
Insider Threat Program Senior Official (ITPSO)	Contractors must appoint a U.S. citizen employee in writing as the ITPSO on the Key Management Personnel (KMP) list in National Industrial Security System (NISS). Separate appointment letters are optional. This individual must have the authority to manage the program and hold a security clearance at the level of the facility's clearance. The Facility Security Officer (FSO) may also serve as the ITPSO; if not, the FSO must be an integral member of the insider threat program team in accordance with NISPOM 117.7(b)(4)(i).
Entity-Wide ITPSO	If an entity family chooses to establish an entity family-wide insider threat program with one ITPSO appointed, each cleared entity using the entity-wide ITPSO must separately appoint that person on its KMP List in NISS. The ITPSO must provide an implementation plan to DCSA for executing the insider threat program across the entity family in accordance with NISPOM 117.7(b)(4)(iii).
Program Function	The program must enable the gathering, integration, and reporting of relevant insider threat indicators. Contractors and their cleared employees are required to report any adverse information or events that could impact an employee's eligibility for access to classified information or indicate a potential threat in

	accordance with NISPOM 117.7(d) and Security Executive Agent Directives (SEAD) 3 and 4.

Required Training:

Contractors can either develop their own training program that includes the required topics outlined in NISPOM 117.12(g) or may use the following existing DCSA CDSE courses to achieve minimum requirements:

Audience	Requirement	Available CDSE Courses	References
Insider Threat Program Personnel	The ITPSO and other individuals managing the insider threat program must complete a one-time specialized training. The ITPSO is responsible for identifying all program personnel at their facility.	"Insider Threat for Industry Curriculum" (INT 333.CU), which includes the following topics: • Protecting Assets (CI117.16) • Mitigation Responses (INT210.16) • Records Checks (INT230.16) • Privacy/Civil Liberties (INT260.16)	32 CFR 117.7(d) 32 CFR 117.12(g) 32 CFR 117.12(g)(1)
All Cleared Employees	All cleared employees must receive initial insider threat awareness training before being granted access to classified information and annually thereafter.	• "Insider Threat Awareness" (INT101.16), **or** • "Counterintelligence Awareness and Security Briefing" (CI112.16)	32 CFR 117.7(d) 32 CFR 117.12(g)(1) 32 CFR 117.12(g)(2)

Training Exemptions:

- **ITPSOs appointed before July 1, 2025:** Must have proof of completing the previous training "Establishing an Insider Threat Program for Your Organization" course (INT122.16) or an equivalent contractor-developed program.
- **ITPSOs reappointed after July 1, 2025:** Must have proof of completing the training "Establishing an Insider Threat Program for Your Organization" course (INT122.16) prior to July 1, 2025.

Additional Resources:

For more detailed guidance, job aids, and best practices, contractors can utilize the following resources:

- CDSE Insider Threat Toolkit: https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/
- National Insider Threat Task Force (NITTF) Maturity Framework: https://www.dni.gov/files/NCSC/documents/features/NITTF_MaturityFramework_web.pdf
- National Industrial Security Program Policy Advisory Committee (NISPPAC) developed Insider Threat Training for Program Personnel slides https://safe.menlosecurity.com/doc/docview/viewer/docN27F85983ED09658591a8d6d751bab4e7f61e7e7a843f2a915b9f32e4bc4a6a7b76d3b6779edd