INSIDER THREAT TRAINING

For Program Personnel

Contractor Responsibility: Contractors must ensure program personnel assigned insider threat program responsibilities complete training consistent with applicable DCSA-provided guidance.

The term “program personnel” refers to those individuals who ***manage*** the insider threat program, including the Insider Threat Program Senior Official (ITPSO). The ITPSO is responsible for identifying specific individuals within their organization who are considered program personnel and therefore subject to these training requirements.

Contractors must also provide insider threat awareness training to all cleared employees prior to granting access to classified information and annually thereafter. Refer to page 2 for more information.

DCSA Responsibility: DCSA will validate those personnel assigned insider threat program management duties, ***as determined by the ITPSO***, have completed the necessary training during initial compliance contacts or the security review process.

Training Options: Contractors under DCSA cognizance have ***three options*** to meet the minimum insider threat program personnel training requirements:

1) **DCSA Designated Training:** Effective July 1, 2025, contractors must use the “Insider Threat Program for Industry Curriculum, INT333.CU.”
2) **Contractor Developed Training:** Create their own training that covers the topics outlined in 32 CFR 117.12(g)(1).
3) **Hybrid Approach:** Combine contractor-developed training with existing DCSA designated courses to cover all the topics outlined in 32 CFR 117.12(g)(1).

Note 1: Insider threat program personnel, including the ITPSO, appointed before July 1, 2025, do not need to retake training.

Note 2: Multiple Facility Organizations who choose to develop their own training can request a DCSA IS HQ review by emailing dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil. Allow 30 days for review.

Note 3: The National Industrial Security Program Policy Advisory Committee (NISPPAC) Insider Threat Working Group is collaborating with DCSA to create an industry-developed training solution. Once available, it will be offered under option 2.

Insider Threat Program for Industry Curriculum, INT333.CU	
32 CFR 117.12(g)(1) Requirements	CDSE Designated Course and Exam
• Counterintelligence and security fundamentals	• Protecting Assets in the NISP, CI117
• Procedures for conducting insider threat response actions	• Insider Threat Mitigation Responses, INT210.16
• Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and the use of records and data, including the consequences of misuse of such information	• Insider Threat Records Checks, INT230.16
• Applicable legal, civil liberties, and privacy policies and requirements applicable to insider threat programs	• Insider Threat Privacy and Civil Liberties, INT260.16

INSIDER THREAT TRAINING

For Cleared Employees

Contractor Responsibility: Contractors must provide insider threat awareness training to all cleared employees consistent with the National Industrial Security Program Operating Manual (NISPOM), specifically 32 CFR 117.12(g)(2). This includes insider threat awareness training initially before granting access to classified information and annually thereafter.

Contractors must establish procedures to validate all cleared employees who have completed initial and annual insider threat training.

DCSA Responsibility: DCSA will validate that cleared personnel have completed the necessary training during initial compliance contacts or the security review process.

Training Options: Contractors under DCSA cognizance have three options to meet the minimum training requirements for cleared employees:

1) **DCSA Designated Training:** Contractors may use either "Insider Threat Awareness, INT101.16," **or** "Counterintelligence and Security Brief, CI112.16."
2) **Contractor Developed Training:** Create their own training that covers the topics outlined in 32 CFR 117.12(g)(2).
3) **Hybrid Approach:** Combine contractor-developed training with existing DCSA designated course to cover all the topics outlined in 32 CFR 117.12(g)(2).

Note 1: Multiple Facility Organizations who choose to develop their own training can request a review by the DCSA NISP Mission Performance Division by emailing dcsa.quantico.dcsa.mbx.isd-nmp-div@mail.mil. Allow 30 days for review.

Insider Threat Awareness, INT101.16 **or** Counterintelligence and Security Brief, CI112.16

32 CFR 117.12(g)(2) Requirements

- Current and potential threats in the work and personal environment
- Importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee
- Methodologies of adversaries to recruit trusted insiders and collect classified information, within information systems
- Indicators of insider threat behavior and procedures to report such behavior
- Counterintelligence and security reporting requirements, as applicable

Insider Threat Programs use multidisciplinary teams who work together to proactively gather, integrate, and report relevant and available information indicative of a potential or actual insider threat. Insider Threat Programs throughout the NISP will vary extensively based on an entity's size and operations. To learn more about insider threat information and resources available, visit the DCSA CDSE Insider Threat Toolkit.