



CONDUCT INSIDER THREAT TRAINING



The designated Insider Threat Senior Official will ensure that contractor program personnel assigned Insider Threat program responsibilities and all other cleared employees complete training considered appropriate by the CSA.

Requirements:

The [NISPOM](#) has identified the following requirements for the Conduct of Insider Threat Training under paragraph 3-103 and [ISL](#) 2016-02.

- Contractor Insider Threat Program personnel, including the contractor designated Insider Threat Senior Official, must be trained in:
 - (1) Counterintelligence and security fundamentals, including applicable legal issues.**
 - (2) Procedures for conducting Insider Threat response actions.**
 - (3) Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information.**
 - (4) Applicable legal, civil liberties, and privacy policies.**

- All cleared employees must be provided Insider Threat awareness training before being granted access to classified information, and annually thereafter. Training will address current and potential threats in the work and personal environment and will include the following information at a minimum:
 - (1) The importance of detecting potential Insider Threats by cleared employees and reporting suspected activity to the Insider Threat Program designee.**
 - (2) Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within information systems.**



(3) Indicators of Insider Threat behavior, and procedures to report such behavior.

(4) Counterintelligence and security reporting requirements, as applicable.

The contractor will establish and maintain a record of all cleared employees who have completed the initial and annual Insider Threat training. Records of training must be available for review during DSS security vulnerability assessments. Records must consist of training attendance records, certificates, or other documentation verifying that personnel required to complete the training requirements have done so. Electronic versions of these items are acceptable.

Getting Started:

Getting started on your Insider Threat Training is as easy as heading over to the DSS Training Directorate, the Center for Development of Security Excellence (CDSE) [website](#). CDSE provides numerous courses on counterintelligence awareness, security fundamentals, and Insider Threat. The "[Insider Threat Awareness](#)" course has been approved by the National Insider Threat Task Force (NITTF) as meeting the minimum standards for initial and annual Insider Threat Awareness Training. "[Establishing an Insider Threat Program](#)" covers essential procedures for setting up shop and addresses many of the requirements for training Insider Threat Program personnel. Consult your legal counsel to enhance training in the areas of gathering, retaining and safeguarding information AND legal, civil liberties, and privacy policies. Your company likely has policies and accompanying training on these issues already in place. Access the CDSE's [Insider Threat Toolkit](#) for more information on Awareness & Training, Policy/Legal, Reporting, Establishing a Program, and Cyber Insider Threat.

Note: Insider Threat Senior Official (ITSO) training must be completed within the 6 month implementation phase. If a new official is appointed after the 6 month implementation period, they must complete the required training within 30-days of being assigned ITSO responsibilities. ITSOs may take CDSE course "Establishing an Insider Threat Program for your Organization" (course CI122.16) in STEPP to receive credit or may develop independent training for the ITSO.

Employee training on insider threat must be taken prior to an employee being granted access to classified information or within 12 months of policy implementation. This training may be part of their initial security briefing and annual refresher training so long as the required topics as outlined in NISPOM 3-103B are covered in their entirety. Records shall be maintained for initial and refresher insider threat training.



Best Practices:

- Designate an Insider Threat Program Group team member, who can also be the FSO, with responsibility for education, training, and awareness. It's a good idea for someone in the program to regularly attend refresher training on new security awareness training topics.
- Remember, while initial and annual refresher training may be the requirement, effective training is not merely an event, but a process. Continue to seek out new sources of information to reinforce learning and awareness of the Insider Threat. [CDSE](#) provides free security posters, job aids, and brochures that are regularly updated.
- Consider Insider Threat awareness training for contractors, vendors, and trusted business partners. An "Insider" is defined as any person with authorized access to any government or contractor resource to include personnel, facilities, information, equipment, networks or systems.

Related Training and Resources:

- eLearning Course for cleared personnel: [Insider Threat Awareness CI121.16](#)
- eLearning Course for Insider Threat Program Personnel: [Establishing an Insider Threat Program for Your Organization CI122.16](#)
- [Insider Threat Training](#)
- [Additional Counterintelligence and Security Fundamentals Training](#)
- Insider Threat Toolkit Tab: [Awareness & Training](#)
- [CDSE Job Aids and Resources](#)