National Insider Threat Special Interest Group (NITSIG)

Insider Threat Awareness Training Resource Guide

Objectives For Insider Threat Awareness Training

- Insider Threat Awareness Training satisfies National Insider Threat Policy (NITP) and NISPOM Conforming Change 2 requirements to educate employees on Insider Threats.
- It raises employee awareness about the indicators of potential insider threats including: erratic or unusual behavior, malicious activity such as data exfiltration, sabatogae, fraud, espionage, unwitting insider threats and knowing violations of company policy. It also provides guidance on how to address insider threats directly when appropriate and when and how to report insider threats.

NITP Requirements

- Provide insider threat awareness training, either in-person or computer-based, to all cleared employees within 30 days of initial employment.
- Or following the granting of access to classified information.
- And annually thereafter.

NISPOM Conforming Change 2 Requirements

- Same As NITP. The contractor is responsible for establishing a system to validate and maintain records of all cleared employees who have completed the training.

Topics That Should Be Addressed

- Define An Insider And The Threats They Could Impose To Critical Assets (Data, Personnel)
- Understand Common Motivations Of Malicious Insiders
- Understand The Different Types Of Insider Threats (Wittingly, Unwittingly)
- Recognize How You Can Become An Unintentional Insider Threat (Violations Of Security Policy)
- Discuss Impacts To Your Government Agency, Business, And National Security (Examples, Why Should I Care?)
- Describe The Consequences / Ramifications Of Being A Malicious Or Unintentional Insider
- Understand How You Can Be Targeted By A Malicious Insider As Well As External Adversaries (Elicitation)
- Identify Reportable Behaviors / Indicators Of Malicious Insiders threats
- Understand Counterintelligence And Security Reporting Requirements (DoD Directive 5240.06)
- Identify Steps You Can Take To Protect Yourself (Active Shooter)
- Be Aware Of Actions To Take If You See Or Suspect An Insider Threat
- Know The Different Ways To Report An Insider Threat (Tip Line, E-Mail, Web Based, Walk-In, Etc.)
- Insider Threat Awareness Resources Available To Your Organization (Website)

DSS Insider Threat Awareness (Web Based Training)

Description: This course provides a thorough understanding of how Insider Threat Awareness is an essential component of a comprehensive security program. With a theme of, "If you see something, say something" the course promotes the reporting of suspicious activities observed within the place of duty. Using a few case study scenarios, the course teaches the common indicators which highlight actions and behaviors that can signify an insider threat. The instruction promotes a proactive approach to reporting the suspicious activities. The course includes a printable certificate which can serve as evidence that a student completed the course.
http://cdsetrain.dtic.mil/itawareness

Department of Homeland Security (DHS): Insider Threat Awareness Video
https://vimeo.com/50793492

If You See Something, Say Something -Insider Threat Awareness Video (DHS)
https://www.youtube.com/watch?v=2M5oR5K2GD0

DSS Cyber Insider Threat Awareness (Web Based Training)
Description: The technological revolution has changed everything about our lives: how we conduct business, travel, bank, date, and even how we spy. The Cyber Insider Threat Course explores the manifestation of traditional espionage indicators in a cyber-environment, identifies new indicators specifically related to the IT insider threat, and discusses observable and reportable behaviors that help to detect, deter, and neutralize cyber insider threat.
http://www.cdse.edu/catalog/webinars/cyber-security/cyber-insider-threat.html

DSS Adverse Information Reporting Guidance
DSS NISPOM Adverse Information Reporting Requirements Presentation
http://www.cdse.edu/documents/toolkits-insider/adverse-information-reporting-march-2014.pdf

DSS NISPOM Reporting Requirements Guide
http://www.cdse.edu/documents/cdse/CDSE_RR_JobAid.pdf

DSS Adverse Information Reporting Resource Toolkit
http://www.cdse.edu/toolkits/fsos/reporting.html

Cleared Employee Reporting Requirements Sign
www.isac-greaterla.com/docs/reportingrequirementsflyer.doc

DSS Potential Espionage Indicators - Detecting Actions Outside the Norm (Web Based Training)
Description: This course will identify and explain indicators displayed by some of the most damaging spies in the U.S. intelligence community's history. Two case studies will be reviewed to see if you can pick out the indicators that should have been reported. The goal is to raise awareness in the cleared contractor and federal sectors with a goal of stopping the next major spy case before it starts.
http://www.cdse.edu/catalog/webinars/counterintelligence/potential-espionage-indicators.html

DSS NISP Reporting Requirements Training Course (Web Based Training)
Description: The NISP Reporting Requirements course introduces the reporting requirements as outlined in NISPOM 1-300. The course covers the structure of the NISP and the relationships between organizations administering and participating in the NISP. Additionally, the course discusses the reporting requirements for changed conditions affecting the facility security clearance (FCL), personnel security clearances (PCL), and safeguarding, as well as reports for security violations and espionage, sabotage, terrorism, and subversive activities. The course examines the typical reporting procedures and the potential impact on the contractor's overall security program.
http://www.cdse.edu/catalog/elearning/IS150.html

DSS Counterintelligence Awareness And Reporting Course For DoD Employees (Web Based Training)
Description: Department of Defense (DoD) Components are required by DoD Directive 5240.06 to provide Counterintelligence Awareness and Reporting training to all personnel within 90 days of initial assignment, or employment to the Component, and every 12 months thereafter. When an experienced Counterintelligence Agent is not available to provide such training in person, this web-based training may be used to meet the training requirement.
http://www.cdse.edu/catalog/elearning/CI116.html

DSS Insider Threat Brochure
http://www.dss.mil/documents/ci/Insider-Threats.pdf

DSS Security Poster- Insider Threats
http://www.cdse.edu/resources/posters.html

DSS Elicitation Brochure
http://www.dss.mil/documents/ci/Elicitation.pdf

FBI Brochure - The Insider Threat: A Guide To Detecting And Deterring An Insider Spy
https://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure

DSS Active Shooter Awareness Web Based Training
http://www.cdse.edu/multimedia/shorts/active-shooter/mod1/module.htm

Terminal Risk Economic And Industrial Espionage Awareness Videos
Terminal Risk is an NCSC training and awareness tool designed to support corporate executives and US industry, helping them to avoid threats and stop economic and industrial espionage. Produced as a series of vignettes, Terminal Risk highlights threats ranging from "Targeting Executives Overseas" to "Office Equipment Exploitation.
http://www.ncsc.gov/index.php

Please e-mail me any additional Insider Threat Awareness Training not listed in this document.

Contact Information
Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense, TopSecretProtection.Com, Inc.
Counterespionage-Insider Threat Program Training Course Instructor
Cyber Security-Information System Security Program Management Training Course Instructor
Cyber Threat-Insider Threat Risk Assessment Auditor / Analyst
Founder / Chairman Of The National Insider Threat Special Interest Group
888-363-7241 / 561-809-6800
www.insiderthreatdefense.com
jimhenderson@insiderthreatdefense.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org