Center for Development of Security Excellence

CDSE

INSIDER THREAT JOB AID

LEARN. PERFORM. PROTECT.

FACILITATION GUIDE

Insider Threat Vigilance Series Episode Four: "Meeting of the Minds"

Overview:

The Insider Threat Vigilance Video Series aids the workforce in identifying and reporting insider threat indicators. The series also provides an overview of Insider Threat Programs and their multi-disciplinary approach to gathering and reviewing information indicative of an insider threat, referring that data as appropriate, and developing mitigation response options while protecting the privacy and civil liberties of the workforce. The goal of the program is to deter threats and detect potential issues early on—before a problem occurs.

This guide will aid you in presenting the Insider Threat Vigilance video to your training audience. Use the questions below to assist with your group discussion. You can access the episode on YouTube or in a micro-learning module with expanded information and resources.

YouTube Location: https://youtu.be/RZHQW3d819M

Micro-Learning Location: https://www.cdse.edu/micro/vigilance-episode4/vigilance-episode4.html

Instructions

Play the video for your group and consider asking the following questions:

Question 1: Where might the agency have to report Joyce's unauthorized disclosure?

Desired Responses:

- Department of Defense
- Congress
- Federal Bureau of Investigation

Question 2: What role do each of the agencies mentioned play with respect to unauthorized disclosure?

Desired Responses:

- Department of Defense: All serious security incidents involving espionage; unauthorized disclosure to the public media or that is reported to the oversight committees of Congress; special access programs or anything relating to defense operations, systems, or technology likely to cause significant harm or damage to U.S. national security; unauthorized disclosure of Sensitive Compartmented Information (SCI); or egregious security incidents as determined by the DoD Component senior agency official.

- Congressional Oversight Committees: Some authorized disclosures are so serious or of such interest to the public that DoD must report them to Congress. After consulting with the Director of National Intelligence (DNI) and the Director of the Federal Bureau of Investigation (FBI), the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) must report to Congress on behalf of the Secretary of Defense each failure or compromise of classified information that the Secretary of Defense determines is likely to cause damage to national security. The Secretary of Energy must report to Congress each security incident involving unauthorized disclosure of restricted data and/or formerly restricted data.

- Federal Bureau of Investigation: Section 811 of the Intelligence Authorization Action of 1995 (50 US Code 402a) is the legislative act that governs the coordination of counterintelligence investigations between Executive Branch agencies and departments and the FBI. Section 811 referrals are reports that advise the FBI of any information, regardless of origin, that may indicate that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or agent of a foreign power.

Question 3: In addition to the reporting requirement, what other action was mentioned that may occur as a result of the unauthorized disclosure?

Desired Response: Sanctions were mentioned. Those who are responsible for unauthorized disclosure face serious consequences. After the investigation is conducted, commanders and supervisors may consider and impose a wide range of sanctions and actions against those found responsible for unauthorized disclosure of classified information. These consequences can take the form of Uniform Code of Military Justice (UCMJ) sanctions, civil litigation, administrative sanctions, and criminal sanctions. For example, individuals may have their accounts suspended and only reinstated after completion of remedial training.

Additional Discussion: If the group has watched the previous three videos, you may ask them to discuss some of the potential risk indicators displayed in those episodes and discuss what an insider threat program is and why it is important.

Indicators from Previous Episodes:

- Splitting up with his girlfriend and calling off their engagement
- Purchasing an expensive car
- Having mentioned financial difficulties
- Unexpectedly submitting his two week notice
- Discouraged because he did not get the lead programmer position
- Working late, quickly turning off computer screen, and talking quietly to someone on the phone
- Inserting USB thumb drives into systems
- Foreign travel

- Attempts to gain access to information outside of normal scope of duties

Additional Discussion: What is an Insider Threat Program?

- Designed to identify "at risk" individuals and help them off this pathway and toward more positive outcomes.
- Insider Threat Programs often assist with solutions that focus on providing help and resources for those in need.
- Insider Threat Programs are multidisciplinary. They typically include representatives from security, counterintelligence, human resources, law enforcement, cyber, behavioral health, and legal. As a team, the group can look at each situation and best determine how to mitigate risk to the organization, including options that would help get employees onto the right path.

Additional Discussion: This is a good time to ask the group if they know how to report information to their Insider Threat Program. The facilitator should provide contact information for their organizational Insider Threat Program.

Additional Facilitator Resources

Insider Threat Toolkit: https://www.cdse.edu/toolkits/insider/index.php

Counterintelligence Awareness Toolkit: https://www.cdse.edu/toolkits/ci/index.php

DoD Insider Threat Trifold: https://www.cdse.edu/documents/cdse/DoD_Insider_Threat_Trifold.pdf

Insider Threat Case Studies: https://www.cdse.edu/resources/case-studies/insider-threat.html

Customizable DoD Command Briefing: https://www.cdse.edu/documents/cdse/customizable-dod-command-brief-for-insider-threat-awareness.pdf

Security Posters: https://www.cdse.edu/resources/posters.html

Potential Espionage Indicators (PEI): Detecting Actions Outside the Norm Webinar (30 minutes):

https://www.cdse.edu/catalog/webinars/counterintelligence/potential-espionage-indicators.html

Adverse Information Reporting Webinar (30 Minutes):

https://www.cdse.edu/catalog/webinars/industrial-security/adverse-information-reporting.html

Preserving Investigative and Operational Viability in Insider Threat Course (60 minutes):

https://www.cdse.edu/catalog/elearning/INT220.html

Unauthorized Disclosure: Educate Yourself

https://www.cdse.edu/toolkits/unauthorized/educate.html