Center for Development of Security Excellence

CDSE

INSIDER THREAT JOB AID

I know I'm required to provide Annual Insider Threat Awareness Training to my personnel, but is that enough to sustain the awareness and reporting message year round?

Insider Threat Awareness is not a one-time event. By providing frequent reminders in a variety of mediums, you are more likely to increase the vigilance of your personnel and encourage awareness and reporting.

Vigilance Campaign FAQ

Vigilance Campaign Materials

Sample Vigilance Campaign Plan

Insider Threat References

Vigilance Campaign FAQ

What is a Vigilance Campaign?

An Insider Threat Vigilance campaign is an ongoing, continual communication program, using a variety of communication platforms such as posters, videos, briefings, and internet sites to keep Insider Threat Awareness and reporting requirements in the forefront for personnel.

Why do we need a Vigilance Campaign?

Executive Order 13587, NISPOM Change 2, and DoDD 5205.16 mandate annual Insider Threat Training for industry, executive branches, and DoD components. This mandate is typically met by requiring that the same training presentation be viewed and a new certificate of completion be issued annually. This approach frequently leads to participants quickly forwarding through the presentation just to get to the certificate at the end. However, in order to be truly effective, annual training can only be part of the solution. An ongoing, continual campaign using a variety of communication methods is an effective means to help the workforce maintain vigilance against the insider threat.

Successful Insider Threat Awareness training instills in all personnel, both those with clearance and without, a "Vigilance" mindset. In addition to continually reinforcing messages in the annually required Insider Threat Awareness Training, creating a "Vigilance" mindset will constantly refresh and reinforce key Insider Threat concepts.

Is a Vigilance Campaign mandated by Policy or Directive?

While a Vigilance Campaign is not specifically required, Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; the White House National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (" Policy and Standards"), dated 21 November 2012; and the National Industrial Security Program Operating Manual, Change 2 all require annual Insider Threat Awareness Training. DoDD 5205.16 also mandates annual Insider Threat Training for all DoD employees, contractors, and volunteers. A Vigilance Campaign should supplement and enhance the required annual training.

What are the goals of an Insider Threat Vigilance Campaign?

The Insider Threat Vigilance Campaign is built on the foundation of required annual training in Insider Threat Awareness as required by Executive order and DoD policy. This annual training must be completed and documented by all employees and contractors. However, once-a-year training is not enough to keep the risks and potential damage at bay. For any Insider Threat program to be fully successful, it must keep the awareness message first-and-foremost in the mind of the workforce. To achieve this objective, the Vigilance Campaign must achieve several goals, including ease of implementation; short duration; frequent repetition; consistent messaging; varying presentation methods so as to appear different to the user each time; tailored to the workforce; and reinforcing reporting requirements and

contact points.

Who is affected by the Vigilance Campaign?

Audiences identified for Insider Threat Vigilance Campaign materials include: personnel; privileged and trusted users of information; organization leaders; and the general workforce.

How can I implement a Vigilance Campaign?

This document provides guidance for developing an Insider Threat Vigilance campaign for the individual DoD component or agency, cleared industry facility, or other organization. This implementation plan includes suggested ways to leverage tools found in the CDSE Insider Threat Vigilance Campaign tab located at:

http://www.cdse.edu/toolkits/insider/vigilance.html

In addition to the sample implementation plan, consider additional options to enhance messaging and awareness at your organization:

- Insider Threat Awareness Day – Forum or meeting featuring guest speakers and leadership, informational briefings, and Q&A sessions with the Insider Threat Program
- Insider Threat Awareness Month – Does your organization feature different topics on a monthly basis? Make sure Insider Threat is among those highlighted.
- Poster or Messaging Theme Contests
- Mobile Applications, Videos, and other graphic heavy platforms to keep the message in the forefront
- Elevator Speech – everyone in the Insider Threat Program should be prepared to offer a concise message about your program in three minutes or less.

What resources are available to help me sustain a Vigilance Campaign?

CDSE has created resources that can be used to develop the "Vigilance" mindset in all members of your organization. These "Vigilance" materials are available from within CDSE's Insider Threat Toolkit. The CDSE Insider Threat Vigilance Toolkit Tab:

- Leverages CDSE's existing resources for security professionals
- Curates additional resources from throughout the Insider Threat community
- Is a dynamic toolset that is frequently updated with newly developed items
- Is easily accessible
- Is user-friendly, engaging, and adheres to DSS PAO guidance

Click here to find materials for use in your campaign.

Back to Top

CDSE has partnered with the OUSD(I) Insider Threat Program Office and DITMAC to ensure materials are consistent with communications and messaging guidance for DoD Enterprise Insider Threat Programs. Click here for additional materials developed for DoD Component Insider Threat Programs hosted on the DITMAC website: https://intelshare.intelink.gov/sites/ditmac

All organizations should consult with their Public Affairs Office prior to releasing materials.

Can I customize Vigilance Campaign materials to make them Component or Agency-specific?

All of the resources produced by CDSE are copyright free. So feel free to customize as you see fit for your audience.

Sample Implementation plan.

All materials available here

Month	*Event*
January	**New webpage banner** **Insider Threat Case Study: Charles Eccleston** **Video: Don't Be a Pawn: A Warning to Students Abroad**
February	**New Insider Threat Poster - Not all Insider Threats are this obvious… (Awareness)** **Insider Threat Case Study: Mostafa Awwad** **Pamphlet: Workplace Violence**
March	**New Job Aid - Foreign Intelligence Entity Targeting Recruitment Methodology** **Insider Threat Case Study: Walter Liew** **Video: Insider Threat Training Scenarios**
April	**New webpage banner** **New Insider Threat Poster - In Trouble? (Self Reporting)** **Insider Threat Case Study: Wen Chyu Liu**
May	**Insider Threat Case Study: Bryan Underwood** **New Job Aid - Spotting Insider Threats** **Video: Voices of the Betrayed**
June	**New Insider Threat Poster - They don't wear nametags (Reporting)** **Insider Threat Case Study: Yuan Li** **Pamphlet: Insider Threat Tri-fold**

July	**New webpage banner** **Insider Threat Case Study: Christopher Boyce** **Video: Intriguing Insider Threat Cases - Make Sure This Doesn't Happen to You!**
August	**New Insider Threat Poster - Make the right choice (Employee Assistance Programs)** **Insider Threat Case Study: Robert Mo** **Video: The CERT Top 10 List for Winning the Battle Against Insider Threats**
September	**New Job Aid - Foreign Collection Methods: Indicators and Countermeasures** **Insider Threat Case Study - Hannah Robert** **Micro -- learning: Overworked**
October	**New webpage banner** **New Insider Threat Poster - Not on my watch (Reporting)** **Insider Threat Case Study - Kun Chun**
November	**Insider Threat Case Study - John Beliveau** **Job Aid – Insider Threat Crossword Puzzle**
December	**New Insider Threat Poster - The biggest threat: Failing to pay attention (Awareness)** **Case Study – James Wells**

Insider Threat References

Department of Defense Directive 5205.16 - The DoD Insider Threat Program

Executive Order 13587 - Structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information

Insider Threat Program Requirements for Industry

Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Dated Nov. 21, 2012)

Back to Top