Center for Development of Security Excellence

CDSE

COUNTERINTELLIGENCE JOB AID

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

Counterintelligence 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

Counter-intelligence References

Counterintelligence Vigilance Campaign FAQ

What is a Vigilance Campaign?

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

Why do we need a Vigilance Campaign?

Department of Defense Directive 5240.06 (DODD 5240.06), Counterintelligence Awareness and Reporting (CIAR); and the National Industrial Security Program Operating Manual, Change 2 mandate annual Counterintelligence Training for industry and DoD personnel. 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 threat posed by Foreign Intelligence Entities.

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

Is a Vigilance Campaign mandated by Policy or Directive?

While a Vigilance Campaign is not specifically required, DODD 5240.06 and the National Industrial Security Program Operating Manual, Change 2 require Counterintelligence Awareness Training. A Vigilance Campaign should supplement and enhance the required annual training. Industry partners not subject to the DODD 5240.06 may still find useful information within the Directive that supports CI Awareness at their facilities.

What are the goals of a Counterintelligence Vigilance Campaign?

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 that could benefit from Counterintelligence Vigilance Campaign materials include: security personnel; privileged and trusted users of information; organization leaders; and the general workforce.

Back to Top

How can I implement a Vigilance Campaign?

This document provides guidance for developing a Counterintelligence 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 Counterintelligence Toolbox located at: https://www.cdse.edu/toolkits/ci/index.php

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

- Counterintelligence Awareness Day – Forum or meeting featuring guest speakers and leadership, informational briefings, and Q&A sessions with Counterintelligence experts
- Counterintelligence Awareness Month – Does your organization feature different topics on a monthly basis? Make sure Counterintelligence 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 – Security and CI professionals should be prepared to offer a concise message about your counterintelligence program in three minutes or less.

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

CDSE has resources that can be used to help develop a "Vigilance" mindset among members of your organization. These "Vigilance" materials are available from within CDSE's Counterintelligence Toolkit. The CDSE Counterintelligence Vigilance Toolkit:

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

Click here to find materials for use in your campaign.

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.

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

Back to Top

Center for Development of Security Excellence - Counterintelligence Campaign

Sample Counterintelligence Vigilance Implementation plan.

All materials available here

Month	*Event*
January	***You are the First Line of Defense***
	Video: CI Awareness **Poster: Hero** **Webinar: Counter-proliferations**
February	***Foreign Recruitment***
	Poster: Online Elicitation and Recruitment **Job Aid: Foreign Intelligence Entity Targeting Recruitment Methodology** **Learning Short: Social Networking**
March	***Foreign Collection Methods***
	Poster: Foreign Collection Methods **Job Aid: Foreign Collection Methods: Indicators and Countermeasures** **Job Aid: Counterintelligence Trivia Twirl**
April	***Supply Chain Risk Management***
	Video: Know the Risk - Raise Your Shield: Supply Chain Risk Management **Brochure: Exploitation of Global Supply Chain** **Toolkit Tab: CI Awareness – Supply Chain Risk Management**
May	***Protecting Defense Technology***
	Job Aid: Industrial Base Technology List **Publication: DSS Technology Trends** **Short: Critical Program Information**
June	***Reporting Requirements***
	Poster: Report All Suspicious Activity **Pamphlet: Reporting the Threat brochure** **Webinar: Critical Elements of a Suspicious Contact Report**
July	***Foreign Travel and Foreign Visitors***
	Short: CI Foreign Travel Briefing **Brochure: Preparing for Foreign Visits** **Brochure: Foreign Travel Vulnerability**

August	***Reporting Questionable Intelligence Activities***
	DoD Whistleblower FAQ **No FEAR Act Reporting** **Guide to Reporting Questionable Intelligence Activity**
September	***Counterterrorism***
	Learning Short: Antiterrorism Force Protection **Job Aid: Suspicious Activity Reporting** **Poster: If You See Something, Say Something**
October	***CI and Cybersecurity***
	Webinar: Cyber Enabled Threats to Cleared Industry **Job Aid: Cyber Threat Case Examples** **Poster: Phishing Awareness**
November	***Economic Espionage***
	Job Aid: Understanding Espionage and National Security Crimes **Poster: Espionage Doesn't Pay** **Insider Threat Case Studies**
December	***CI Awareness***
	Poster: Keep Calm and Call Your CISA **eLearning Game: CI Magic 8-Ball** **Video: Request for Information**

Counterintelligence References

DoD Instruction 5200.39 - Critical Program Information (CPI) Protection Within the DoD
DoD Directive 5240.06 - Counterintelligence Awareness and Reporting (CIAR)
Executive Order 12333 As Amended - United States Intelligence Activities
NISPOM DODD 5220.22-M Incorporating Change 2
ISL 2013-05
ISL 2006-02
DSS Counterintelligence Directorate
CI Awareness Toolkit

Back to Top