DoD Insider Threat Program

– Best Practices –

3.1 Strategic Communications for the Workforce

Rev 2

05/24/2017

The Under Secretary of Defense for Intelligence is the Senior Official for Insider Threat

Do you have any questions, comments, or concerns on this topic or others? Would you like to add your component to this Best Practices Edition?

If so, please contact the DoD Insider Threat Program at **osd.pentagon.ousd-intel.mbx.dod-insiderthreatprogram@mail.mil**

We look forward to updating and revising this edition, by adding other participants.

NOTE: The Best Practices series will deliberately be anonymized so that responses are not attributed to a participating Component with exception to the DoD Insider Threat Management Analysis Center (DITMAC), the Center for Development of Security Excellence (CDSE), and the National Insider Threat Task Force (NITTF). The information in this booklet is offered as guidance. It does not convey a task or directive. Each Component conforms to multiple and varying authorities. As such, each Component needs to confer with their Office of General Counsel (OGC) to verify their procedures conform to legal pronouncements.

Purpose:

The DoD Insider Threat Program has compiled data and information from several selected DoD Components that can offer field tested procedures which have produced credible results. These methods, techniques, and professional procedures are offered to Components to assist in their efforts to improve their respective Insider Threat Program (InTP). All best practices are informational, and individual programs should ensure any implementation actions are in compliance with their Office of General Counsel (OGC) and organizational policies before implementation.

Description:

This edition addresses questions pertaining to how Components developed Strategic Communications for their workforce. Eleven questions were posed to 5 Components. DoD activities (CDSE) participated as well, conveying their role in providing Strategic Communications for their Workforce.

Acronyms:

CI	Counterintelligence	**IC**	Intelligence Community	**PAO**	Public Affairs Office
CBT	Computer Based Training	**InT**	Insider Threat	**PM**	Program Manager
CBTM	Computer Based Training Module	**InTP**	Insider Threat Program	**SOP**	Standard Operating Procedure
DoD OIG	DoD Office of the Inspector General	**InT PM**	Insider Threat Program Manager	**TP**	Talking Point
DITMAC	DoD Insider Threat Management and Analysis Center	**MIG**	Military Intelligence Group		
DSS	Defense Security Service	**NITTF**	National Insider Threat Task Force		
HR	Human Resources	**OGC**	Office of the General Counsel		

Table of Contents

Q1. Does your Component have an organic Public Affairs Officer, and if so, to what end have you engaged with him/her in the development of your Insider Threat communications and outreach strategy for the workforce?

Component #1

Yes we have an organic Public Affairs Office (PAO). We began working with our PAO during the development of our program to assist in the development of messaging both internal to the organization, and to prepare the Agency in case we received external press requests.

Component #2

PAO is a key member of our Hub.

Component #3

Our component has an organic PAO. While we have coordinated and worked with the PAO on Insider Threat materials (brochures, briefings, newsletters, forums, etc.), a strategic Insider Threat communications strategy has not yet been developed. This is an area where we could use some expertise and assistance.

Component #4

Our agency does possess its own organic PAO, referred to as Corporate Communications (Corp Comm). We have engaged with this entity on a few occasions to advertise the new InTP. Our first engagement revolved around orchestrating an interview between Corp Comm and our InT Senior Official. This interview was then 'published' on our intranet for all employees to read. Our second attempt is ongoing and we are hoping to send out a mass email to all employees to alert them to the recently launched InT Computer-Based Training Module (CBTM) (e.g. Defense Security Services (DSS) CBTM).

Component #5

Yes. Additionally, we are exploring engaging Strategic Communications for future InT initiatives.

Q2. What organization(s) were involved in the development of your Component's InT strategic communications for the workforce?

Component #1

We leverage our PAO and Equal Opportunity Office (EOO) in the development of communications and education products.

Component #2

Chief of Staff, Public Affairs, Legal Counsel, Insider Threat Program Manager

Component #3

See response from Q1.

Component #4

The organization the program rests beneath, Enterprise Management Services, and the aforementioned Corp Comm (PAO).

Component #5

Our directorate develops strategic communications related to InT internally. Some communications are coordinated with executive leadership, particularly if it is a new type of message or if it is being sent to the workforce by senior leadership. All Component-wide email messages are vetted by our Component's strategic communications team prior to release.

Q3. Other than mandatory workforce training, does your Component utilize any other strategic communications method to train the workforce to recognize and report a potential Insider Threat, as well as the value of the program?

Component #1

We conduct quarterly brown bags, a quarterly Insider Threat Newsletter, periodic agency-wide communication roundtable messages, various flyers and pamphlets, as well as an unclassified Insider Threat Portal.

Component #2

- Integrated into our Initial Security Briefings
- Annual Counterintelligence Training conducted by an Agent assigned to the 902nd Military Intelligence Group (MIG)
- Integrated into the Annual Security Refresher training
- We have an email box dedicated to receiving possible Insider Threat reports
    - The box is only accessible by the Senior Official and InT Program Manager

Component #3

In addition to our workforce and Hub training requirements, Insider Threat and counterintelligence information is integrated into a variety of training courses (Cybersecurity, Information Security, Counterintelligence (CI), etc.) and disseminated through Computer Based Training (CBTs) courses, newsletters, an Insider Threat webpage, and other informational documents.

Component #4

Training outside of the DSS CBTM is virtually non-existent. We have a plan in place to train all supervisors on the indicators of an Insider, how to report, etc. Furthermore, we have published an Insider Threat Notification Form which is located on the main page of our ePortal intranet. The form is perfectly situated in a location where employees visit frequently. This was a success for our InTP on numerous fronts. We have the ability to post articles in a daily 'newsletter' that is e-mailed out to employees.

Component #5

Yes, we provide a variety of briefings and products (posters/brochures) that are available year-round regarding the CI threat, which includes Insider Threats. We are currently developing a campaign specific to recognizing and reporting Insider Threats. We are expanding our Component outreach with focus groups on this topic.

Q4. Does your Component have an independent "Insider Threat" website? If not, how does your Component get InT information out to the workforce? If your Component does have an independent "Insider Threat" website, can you provide a snapshot of the homepage?

Component #1

Yes, we maintain an unclassified Insider Threat Portal page. The site provides education and awareness, as well as a platform for anonymously reporting potential incidents directly to the insider threat Hub.

Component #2

Yes, our website is available upon request.

Component #3

Yes. Our component has a value added Insider Threat-specific website that provides user friendly information and awareness products. The site also provides a simple capability for employees to report anonymously suspicious Insider Threat activities.

Component #4

On our internal ePortal, we have a webpage where we have contact information, links to references for the InTP, and a link to the training and InT awareness products. Our website is available upon request.

Component #5

Yes, in conjunction with the campaign we are currently working on, a corresponding website is also being developed. In addition to the website, Component-wide messages provide the community information regarding organic Insider Threats.

Q5. Can you describe your Component's InT messaging themes? Are they focused on CI, workplace violence, or self-harm?

Component #1

As far as themes, we have profiled several past offenders – listing the indicators associated with their event. We have also focused on workplace violence, offering indicators on suicide, hostile workplace, etc.

Component #2

Our messaging themes are focused around a combination of those areas.

Component #3

While our current Insider Threat messaging attempts to integrate workplace violence, counterintelligence, antiterrorism, and individual behavior may be viewed as harmful or irregular, one should not consider the current effort a theme. We are taking a holistic view of Insider Threats and applying existing program materials accordingly.

Component #4

No messages have been communicated yet and we are working to develop multiple themes across various venues on a regular basis.

Component #5

Most of our InT messaging themes are related to CI/unauthorized disclosures (including media leaks) or restricted items. Some briefings touch on other issues, like workplace violence or self-harm, however those incidents are primarily handled by Human Resources (HR), who has separate messaging and training. Other InT messaging has occurred on new InT initiatives including IT security changes.

Q6. Does your program offer your workforce the ability to report potential incidents anonymously? If so, how?

Component #1

Yes, through either a toll-free number, and through the Insider Threat Portal.

Component #2

We utilize an Insider Threat mailbox.

Component #3

We have created a simple capability that allows employees to report suspicious activities/behaviors anonymously through an email link established on our Insider Threat webpage. Employees can also report activities directly to the Security Office.

Component #4

Our preference is to not make any reports anonymously. We feel that if people were able to do so we would possibly receive a lot of erroneous 'tips'. Our online notification form does not allow for an anonymous notification.

Component #5

Most reporting avenues are traceable and require the individual's contact information. We do have one feedback form that can remain anonymous; however we do not advertise that as the primary method for reporting InT issues. We find that people frequently leave out pertinent details when initially reporting InT issues online, requiring follow up to begin investigation. Anonymous reporting can be extremely difficult to investigate.

Q7. Does your program have a hotline (online, phone, etc.) that the workforce can utilize to submit reportable events? If so, how does it work? Who or what organization operates, receives, and controls the inquiry (calls, emails, etc.)?

Component #1

Yes, we have a hotline that is maintained by our office.

Component #2

We have an email box dedicated to receiving possible Insider Threat reports that is only accessible by the Senior Official and InTP manager.

Component #3

Our component is currently working on an Agency-level hotline which when completed will allow employees to report a multitude of concerns, to include insider threat concerns. The new hotline will mirror the current DoD Office of the Inspector General (DoD OIG) hotline process.

Component #4

Employees are directed to contact either of the InT analysts directly. Once the InT Program Manager (InT PM) has come onboard, his/her number will be advertised as well. Additionally, we have an InTP centric email address that employees can utilize to contact any InTP personnel. Only the InTP personnel have access to the shared mailbox.

Component #5

Yes, there is an online reporting mechanism for reporting security/CI/suspicions to our directorate's website and our upcoming campaign's website. The online form generates an email which is sent to the CI Staff for appropriate action. Copies are also automatically sent to our analysis Hub for documentation.

Q8. What Insider Threat communication/messaging training do you offer supervisors/managers?

Component #1

Supervisors and managers are provided Insider Threat training as part of their annual supervisor/manager required training. In addition, that training is reinforced through brown bag meetings, and flyers tailored to that demographic.

Component #2

We have an Insider Threat tabletop exercise for our Hub and a separate tabletop exercise for our Senior leaders.

Component #3

None. The need for additional training for supervisory personnel has not been realized at this time.

Component #4

We are developing training to provide at supervisor training/forums that would provide an overview of the program, indicators and behaviors of potential insider threats, and how to make reports to the InTP.

Component #5

Part of our upcoming campaign that is under development will include literature and briefings tailored to managers. We will brief this material in the management training courses for leaders at various levels (front-line, mid-level, seniors). This training is focused on facilitating conversations about the importance of recognizing and reporting potential InT concerns to security, and how a disclosure can negatively impact mission.

Q9. Does your Component have materials you are willing to share with other agencies? Does your Component use posters or flyers?

Component #1

We have posters, pamphlets and flyers. All are available to any organization requesting them.

Component #2

We ordered the posters provided by CDSE.
http://www.cdse.edu/resources/posters-insider-threat.html

Component #3

Our agency encourages information sharing and has provided several agencies various materials (Policies, Standard Operating Procedures (SOPs), Implementation Plans, Non-Disclosure Agreements (NDAs), training materials, etc.) used in the establishment of our current program. In addition, we have an Insider Threat brochure modeled off the CDSE brochure.

Component #4

All of the materials we utilize have come from the DoD, NITTF, or from CDSE. We currently do not utilize posters or flyers.

Component #5

Yes, we are willing to share our posters and brochures.

Q10. Does your Component incorporate case studies into your strategic communications plan?

Component #1

Yes, we routinely use well-known case studies as part of our training and awareness.

Component #2

The case studies are used by our cover Agent from the 902nd MIG during our annual counterintelligence briefing

Component #3

We include a multitude of case studies in our training and awareness products to the workforce. Case studies are tuned to the audience (based on make-up and location).

Component #4

Not at present, however we have given consideration to this. Whenever we are broadcasting the program to leadership we utilize these real-world examples to illustrate the importance of the InTP.

Component #5

We incorporate case studies into our strategic communications for the workforce as best we can. If we have a sensitive case or a case with a pending criminal investigation, we are limited to the information that we can share with the workforce while the investigation is ongoing.

Q11. Has your Component developed InT Talking Points (TPs) for the workforce? If so, could you please provide them?

Component #1

We have a number of desk side briefings used to give a two-minute "elevator talk" to our workforce, manager and supervisors.

Component #2

We have not developed any talking points at this time.

Component #3

Not at this time.

Component #4

We have not established talking points for the workforce.

Component #5

Not related to generic InT, however our PAO does provide TPs to the workforce following significant events, such as the 2013 media leaks.

Q12. For CDSE Only – Does CDSE provide training or materials for Strategic Communications for the Workforce?

CDSE

Yes. CDSE has developed and deployed the 'Vigilance Campaign' that is aimed to instill a sense of vigilance in the general workforce. We consider this to be a basic tenet of establishing an InTP. Annual awareness training is a start, but the message can diminish over time. Developing a vigilance campaign for your organization is an effective solution. Deploying regular messaging, awareness, and communications materials ensures that the general workforce is prepared to recognize and respond to the Insider Threat. This campaign can also serve as an introduction to your InTP, ensuring that everyone knows whom to report to and feels comfortable doing so. 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. Visit the following link to access all materials and additional information pertaining to the 'Vigilance Campaign':
http://www.cdse.edu/toolkits/insider/vigilance.html

Q13. Where can components find the materials, job aids, and key information pertaining to strategic communications aforementioned in this Best Practices edition?

OUSD (I)

There are some excellent materials developed by Components throughout the enterprise. If you are interested in any of the posters, brochures, or other key information pertaining to strategic communications in this Best Practices edition, please contact the DoD Insider Threat Program and we will provide you contact info. Participating Components have stated that they are willing to share their programs materials to those InTPs that reach out directly.

Attachment(s)

CDSE – Vigilance Campaign Guidance

Attachment(s) are on the following pages

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