



# CDSE

Center for Development  
of Security Excellence

## Insider Threat Webinar Series

**PERSONNEL AND SECURITY RESEARCH CENTER:  
MAXIMIZING ORGANIZATIONAL TRUST**

LEARN.  
PERFORM.  
PROTECT.

# ***Today's Session:***

**Host:**

**Rebecca Morgan, CDSE Insider Threat**

**Guests:**

**Ms. Stephanie Jaros, PERSEREC**

**Dr. David Prina, PERSEREC**



**CDSE**

Center for Development  
of Security Excellence

Enlarge Screen

Polls, Chats and Feedback



Q & A

Chat Q2 - Shorts

What shorts have you found most helpful? or What shorts do you think might be beneficial to you and your security program?

Type your answer here...

Poll #1

View Votes

How many s  
Process

3

4

5

6

No Vote

Feedback 3

Type your unclassified comments here. Both positive and constructive comments are useful. Suggestions: How do you actually use what was presented on the job? What changes would improve your webinar experience?

Type your answer here...

File Share



# INTRODUCTION



- **Malicious insiders pose a threat to every organization**

- Nadal Hasan – Fort Hood shooting (2009)
- Aaron Alexis – Navy Yard shooting (2013)
- Reality Winner – Intelligence disclosure (2018)



- **Within the Federal Government, Insider Threat Programs have been set up in response to these incidents in order to protect the organization and its members**

- Executive Order 13587
- DoDD 5205.16 “The DoD Insider Threat Program”

*Everyone* is responsible for protecting each other and the organization, not just the Insider Threat Program

Insider Threat Programs cannot succeed without people who are willing to participate!

# PARTICIPATION IN REPORTING

## OBSERVATION

Much of the most meaningful Insider Threat information comes from people who observe and report the behavior of others

## PARTICIPATION IS NOT GUARANTEED

People often have to overcome barriers to reporting, like potential stigma or personal connections with other coworkers

Participation is dependent upon multiple factors, but an important factor is *trust*:

- The organization will handle reported information *responsibly* and *confidentially*
- The deliberative *process* of handling the “case” is done *fairly*
- The outcome of any deliberation is *adjudicated fairly*

**Q:** Why may reporting adverse information on a close friend or colleague be difficult?

**Q:** Why may reporting adverse information on yourself be difficult?

# TRUST AND PARTICIPATION

Insider Threat Programs ask people to think about the **safety of the organization** and require employees to take the (sometimes) **difficult step of reporting** on themselves or others.



If there is no trust in the fairness of the reporting process or outcomes, the personal consequences of reporting become priority over the safety of everyone:

- “If I report Joe’s binge-drinking, will he find out I reported him?”
- “I saw how management reacted when they heard Jack was taking depression medication, so I’m going to stay silent about my own problems.”
- “If I report my financial troubles, will I lose my clearance or my job, and make my situation even worse?”



People need to trust that leadership will take **fair and appropriate** action

# FILLING THE TRUST GAP



DoD SMEs and experts in security management said....

An Insider Threat program is not just a “catch the bad guy” program, but ideally will improve “organizational wellness”

Leaders must foster a positive workplace culture, communicate concerns up and down the organization, and have the courage to make difficult decisions

“Keep butts in seats, not throw them to the street”

Leaders need to know how to listen and how to have difficult conversations

# FILLING THE TRUST GAP

## Purpose

Connect the concept of organizational trust to the needs of Insider Threat Programs

Give leaders and security managers insight into building and maintaining trust

Reinforce safety as a collective responsibility

## Audience

Leaders and security managers within the military, government, and industry

Anyone with an Insider Threat Program

## Challenges

How do we create a product that is applicable/generalizable to such a large audience?

How do we merge Insider Threat concepts with organizational trust?

# THE TRUST GUIDE PRODUCT

The Guide takes the audience through a hypothetical but realistic scenario involving a new commander tackling a possible insider threat issue.



## Sam

Sam is an older man with a history of aggressive behavior, health issues, and a troubled family who causes harm to the organization and its mission.

In many cases, concerning behaviors are correctable and do not stem from an intent to do harm (e.g. ignorance, neglect, unintentional risky behavior etc.). Often, leaders can address these concerning behaviors early, and put the individual on a more productive path.



## Captain Jordan

The Guide follows Captain Jordan as she becomes aware of, and tries to address the behavior of a troublesome employee.

As the guide goes on, we learn Sam's behavior has been ignored by leadership despite complaints by co-workers.

His behavior stems from significant life stressors and was reinforced by years of bad leadership practices and inaction.

# THE TRUST GUIDE PRODUCT

## Captain Jordan is faced with a crisis

Another co-worker, Carla, brings a weapon into the workplace and cites safety concerns working with Sam

Sam's behavior leads to other bad behavior in the organization

## Response to behavior

Captain Jordan works with the group to formulate an appropriate response: document any behavior and actions, discipline Carla and offer Sam relevant employee assistance programs to bring his temper under control.

## Insider Threat Working Group



Captain Jordan convenes an Insider Threat Working Group made up of: Legal, Human Resources, Employee Assistance Program, Security, and Management.

Collaboration between leaders and individuals with diverse expertise creates better responses and better outcomes.

# THE TRUST GUIDE PRODUCT



Sam rejects the offer and behaves aggressively towards his supervisor. Sam storms out and security is alerted.



Security finds that he has been improperly storing classified information.

Sam is **denied** further access to the facility.

Captain Jordan holds all-hands meeting to discuss new changes to reporting and security.

The office mood improves, and there is a drastic reduction in employee turnover.

While not an ideal ending, the guide highlights that a prior pattern of inaction and inappropriate leadership responses led to a bad situation becoming worse.

Earlier intervention could have prevented Sam's behavior and later Carla's weapon.

The guide does not want to sugar-coat the responsibility of leadership – sometimes taking action is difficult but necessary.

# LESSONS OFFERED

We wanted to offer our audience lessons on how to build and maintain trust through careful and considered action

## Lessons for Leaders

- Transferring or waiting until a troubled employee is no longer your responsibility simply transfers the trouble to someone else – maybe making the situation worse
- Positive feedback for taking action – mission performance increases afterwards
- Collaboration across all levels makes for better responses

## Lessons for Security Managers

- Insider threat is not just about “catching the bad guy”
- Get ahead of incidents with policies and training, and follow them
- How to collaborate across all levels to create better responses

# TAKEAWAYS

## Takeaways

- **As the story progresses, the audience also learns about three concepts from industrial/organizational psychology that contribute to trust**
  - Organizational Identification
  - Job Involvement
  - Job Satisfaction
- **These concepts, and how they look in practice, can help leaders and security managers identify maximize trust**

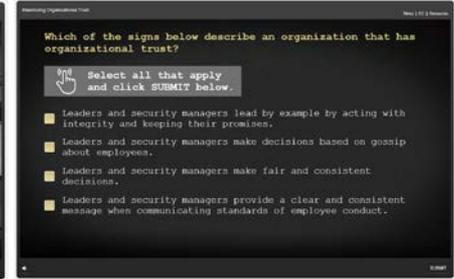
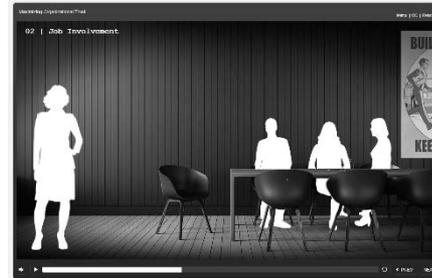
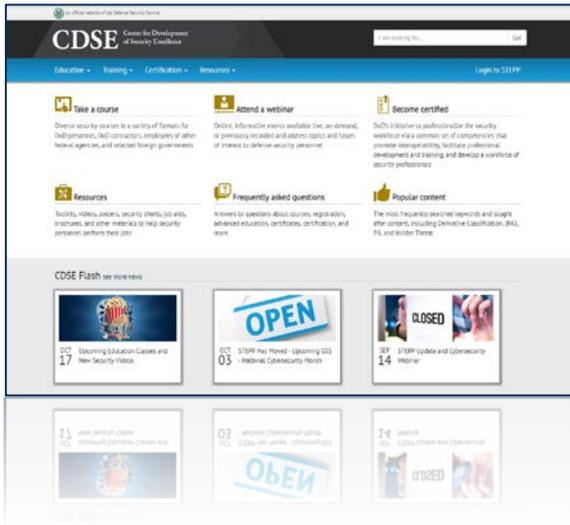
## Follow-on Materials

Printable posters, other composite case studies, and follow-on guidance.



# THE TRUST GUIDE PRODUCT

Hosted on CDSE.edu





OFFICE OF PEOPLE ANALYTICS

**PERSEREC**

DEFENSE PERSONNEL AND SECURITY RESEARCH CENTER

# For More Information

Stephanie L. Jaros

Project Director

[Stephanie.L.Jaros.civ@mail.mil](mailto:Stephanie.L.Jaros.civ@mail.mil)

[www.dhra.mil/perserec/](http://www.dhra.mil/perserec/)

January 2019

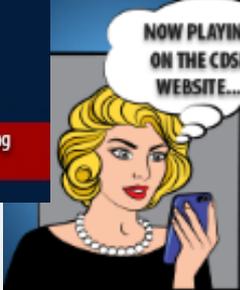
# NEW INSIDER THREAT TRAINING



**NOW PLAYING  
ON THE CDSE WEBSITE...**

**INSIDER THREAT VIGILANCE SERIES  
EPISODE 1: "AN ODD ENCOUNTER WITH TIM"**

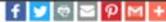
The Insider Threat Vigilance Series aids the workforce with understanding how to identify and report potential risk indicators.



**NOW PLAYING  
ON THE CDSE  
WEBSITE...**

**INSIDER THREAT VIGILANCE SERIES  
Episode 2: "Turning People Around,  
Not Turning Them In"**

The Insider Threat Vigilance Series aids the workforce with understanding how to identify and report potential risk indicators.

"Check Out My New Ride," Season One: Turning People Around, Not Turning Them In. 

[Home](#) [Resources](#) [Security Training Videos](#) "Check Out My New Ride," Season One: Turning People Around, Not Turning Them In

MAJ Montenegro considers Tim over a recent break-up with his ex-fiance. Tim discusses a few changes to his lifestyle that concern MAJ Montenegro. Watch the video, and place yourself in MAJ Montenegro's shoes. What would you do, and why?

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 all 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. Click the links to learn more.



Episode 2 — "Check out my new Ride"

Watch later Share

Watch

- Think
- Dig Deeper
- Question



# CDSE

Center for Development  
of Security Excellence

# INSIDER THREAT TRAINING RESOURCES

## eLearning

- Establishing an Insider Threat Program
- Insider Threat Awareness
  - Available on Multiple Training Platforms: STEPP, Open eLearning, AGILE

## Webinars/Shorts

- Behavioral Science in Insider Threat
- The Defense Insider Threat Management Analysis Center
- Speaker Series with OUSDI Leadership
- Cyber Insider Threat
- And many more...

## Job Aids

- Insider Threat Case Studies
- Understanding Espionage & National Security Crimes
- Foreign Intelligence Targeting & Recruitment
- Insider Threat Job Aids for Industry
- And many more...

## Toolkits

- Insider Threat
- Personnel Security Adjudicator
- Unauthorized Disclosure

The collage displays various training materials from the Center for Development of Security Excellence (CDSE). It includes:

- An eLearning module titled "Insider Threat Awareness" featuring a man with glasses.
- A poster for the "INSIDER THREAT PROGRAM (ITP) FOR INDUSTRY" with a woman in a business suit and a man in a blue shirt.
- A video player showing a webinar with a panel of speakers.
- A "High Profile Examples" document listing several cases, such as "November 5, 2009 - Sony Music sold music files to 12 and ripped 30 others at her house, TX" and "May 27, 2009 - Sony Music: Bradley Manning arrested for leaks involving 1,000,000 classified documents".
- A "Job Aid" titled "Awareness in Action: Case Study" featuring Wen Chyu Liu, a former research scientist at Dow Chemical Company (1965-1992), and a list of espionage indicators: Unexplained Affluence and Foreign Contacts.
- A "toolkit" for mobile devices with icons for Awareness & Culture, Data Guard, Research, Workflows & Forms, and User Access Control.



## **Insider Threat Training POC:**

**Rebecca Morgan**

**(410) 689-1294**

**Email: [Rebecca.a.morgan22.civ@mail.mil](mailto:Rebecca.a.morgan22.civ@mail.mil)**



**CDSE**

Center for Development  
of Security Excellence