



CDSE

Center for Development
of Security Excellence

Insider Threat Webinar Series

**The Resource Exfiltration Project: Findings from
DoD Cases, 1985-2017**

**LEARN.
PERFORM.
PROTECT.**

Today's Session:

Host:

Tom Gentle, CDSE Insider Threat

Guests:

Ms. Stephanie Jaros, PERSEREC

Ms. Katlin Rhyner, PERSEREC



CDSE

Center for Development
of Security Excellence





OPA
OFFICE OF PEOPLE ANALYTICS

PERSEREC
DEFENSE PERSONNEL AND SECURITY RESEARCH CENTER

The Resource Exfiltration Project: Findings from DoD Cases, 1985-2017

Stephanie L. Jaros & Katlin J. Rhyner

January 2019

THE CHALLENGE



THE CHALLENGE: “Loss of our secrets whether through espionage, theft or unauthorized disclosure for other reason – will never be eliminated, but the opportunities therefor can be diminished and attempts at compromise made more difficult at acceptable – indeed modest – cost.”

RECOMMENDATION: “Establish a policy that all persons entering or leaving defense activities, including, to the extent practical, its contractors, are subject to inspection of their briefcases and personal effects, to determine if classified material is being removed without authority.”

- The Stilwell Commission Report (1985)

THE CHALLENGE PERSISTS



“If you have a bag full of stuff, you’re probably going to get stopped.’ . . . But, in general . . . ‘Disneyland has more physical security checks than we had.’”

- NSA Employee, In response to Harold Martin exfiltration (2016)

Photo from Indiana Daily Student,
<http://www.idsnews.com/article/2016/10/prosecution-of-whistleblower-demonstrates-govt-overreach>

Quotation from The Washington Post,
https://www.washingtonpost.com/world/national-security/nsa-contractor-thought-to-have-taken-classified-material-the-old-fashioned-way/2016/10/12/ffc25e22-8cb1-11e6-875e-2c1bfe943b66_story.html?utm_term=.ea914e2d853b

THE HUMAN PROBLEM



“Where we’re missing the boat, oftentimes, is on the human resource side. . . . At the end of the day, what we have to realize is, we’ll never stop the insider threat. The goal is to stop them before he or she decides to. We have to find a way to identify, mark them ahead of time and say, ‘hey listen, I know things are rough, you’re having problems, but there’s other options.’”

- William Evanina, Director, National Counterintelligence and Security Center (2017)

Quotation from Meritalk.com,
<https://www.meritalk.com/articles/insider-threat-programs-miss-human-side-problem-bill-evanina-odni-cybersecurity/>



INSIDER THREAT RESEARCH PRINCIPLES

- A person's transformation from a trusted employee to an insider threat is a process, not an event.
- Insider threats occur in a social context—certain environments are more likely to facilitate insider threat behavior.
- The risk of becoming an insider threat is not randomly distributed throughout the workforce—certain people are more likely to pose threats.
- High-impact, low frequency insider threat behavior is correlated with and preceded by far more common behavioral indicators that can be observed, modeled, and potentially mitigated.

INSIDER THREAT BEHAVIORAL INDICATORS

Gambling problems **Adultery** Unexplained absenteeism Unusual interest in weapons **Threatening communications** Requesting information without a need-to-know Criminal behavior **Extensive use of equipment to reproduce or transmit material** Installing unauthorized software Asking for a colleague's password **Leaving a safe open** Discussing classified information in a public setting Removing classification markings from documents **Anti-U.S. comments** Decline in work performance Working too much **Working too little** Hostile behavior Unreported foreign travel and/or foreign contacts **Drug and/or alcohol abuse** Divorce Physical illness **Bankruptcy** Financial affluence Bizarre behavior



THE RESOURCE EXFILTRATION PROJECT

- Revised eligibility criteria to focus on the incident rather than the prosecution
 - Include spies, leakers, hoarders
 - Include classified and unclassified government resources
- Revised codebook
 - Create a reliable, valid data set
 - Identify individual intervention points
 - Identify organizational gaps and vulnerabilities



THE RESOURCE EXFILTRATION PROJECT

ADJUDICATIVE GUIDELINES

- A: Allegiance to the U.S.
- B: Foreign Influence
- C: Foreign Preference
- D: Sexual Behavior
- E: Personal Conduct
- F: Financial Considerations
- G: Alcohol Consumption
- H: Drug Involvement
- I: Psychological Conditions
- J: Criminal Conduct
- K: Handling Protected Information
- L: Outside Activities
- M: Use of IT Systems

ADAPTED THREAT ASSESSMENT CATEGORIES

- Concerning Communications
- Concerning Interests
- Planning Behavior
- Significant Life Events
- Concerned Others

THE RESOURCE EXFILTRATION PROJECT

PERPETRATORS

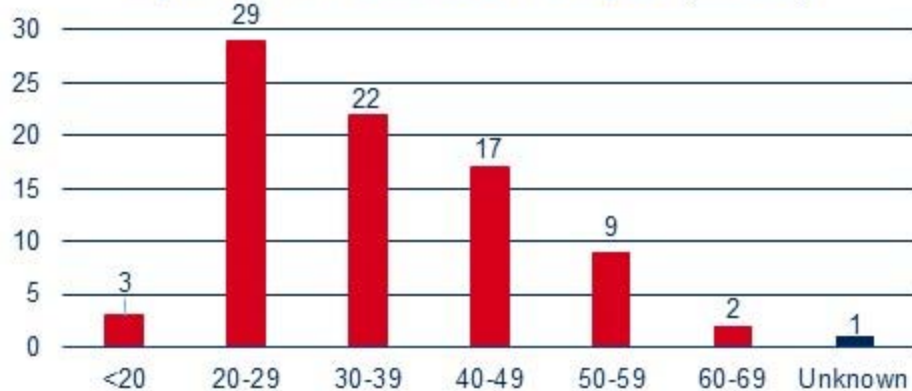
- 83 people
- Exfiltrated a DoD resource
- Arrested after November 19, 1985
- Convicted or pled guilty by December 31, 2017

CODEBOOK

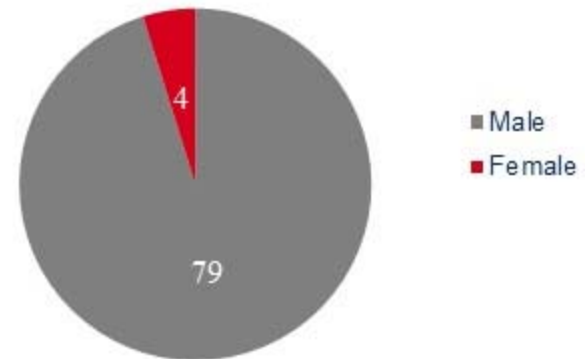
- 392 variables organized into 8 sections
- Demographic
- Employment
- Initiation
- Exfiltration
- Judicial Outcome
- Motive
- Adjudicative Guidelines
- Behavioral Threat Assessment

RESULTS: THE WHO

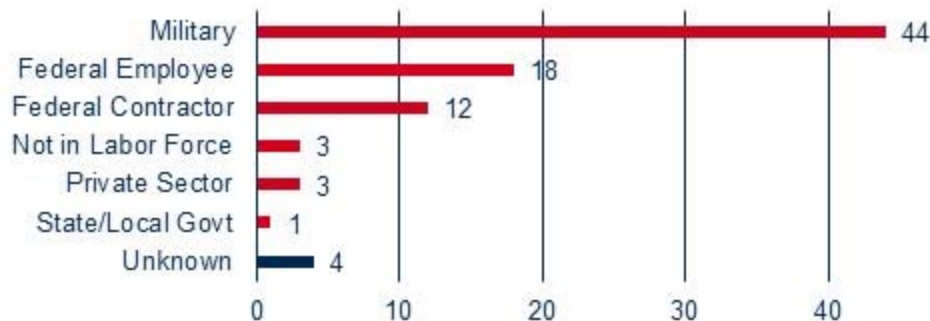
Age When Exfiltration Began (N=83)



Sex When Exfiltration Began (N=83)



Occupation When Exfiltration Began (N=83)



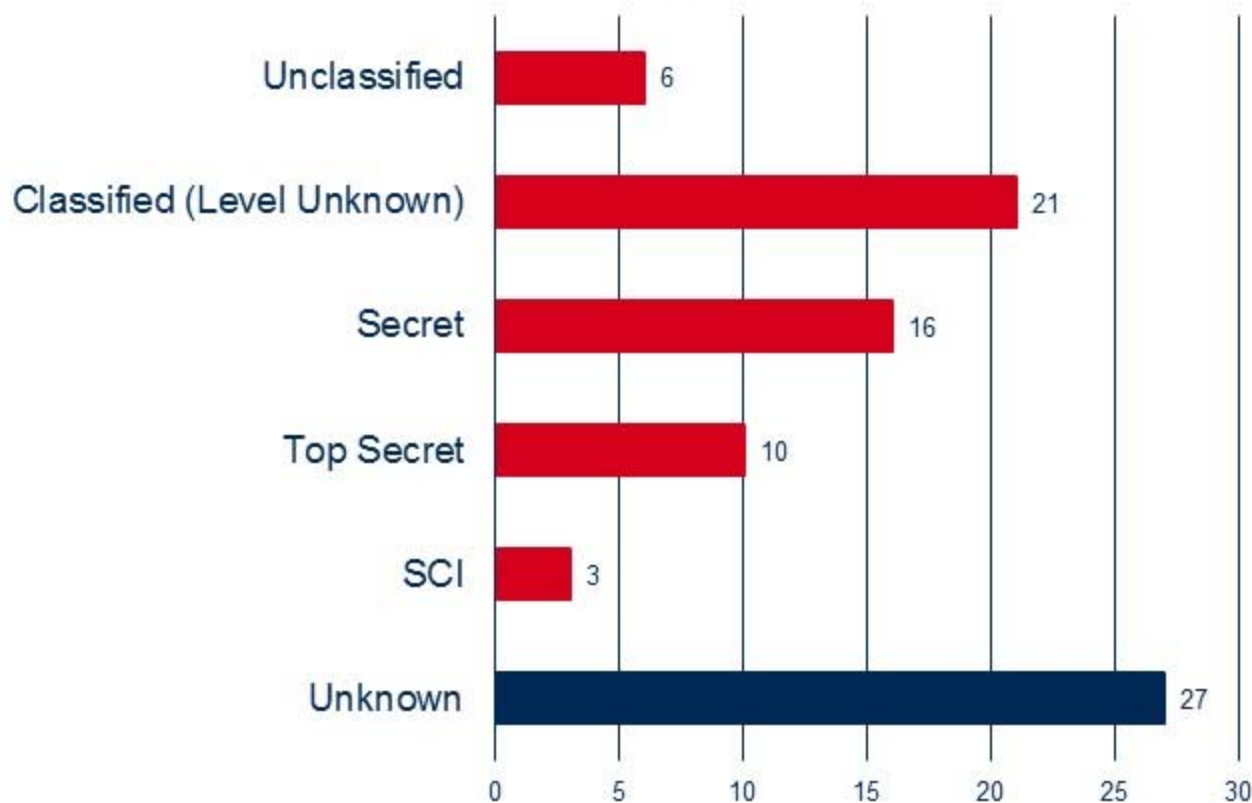
Total exceeds 83 because two perpetrators had multiple occupations when exfiltration began

Citizenship When Exfiltration Began (N=83)



RESULTS: THE WHAT

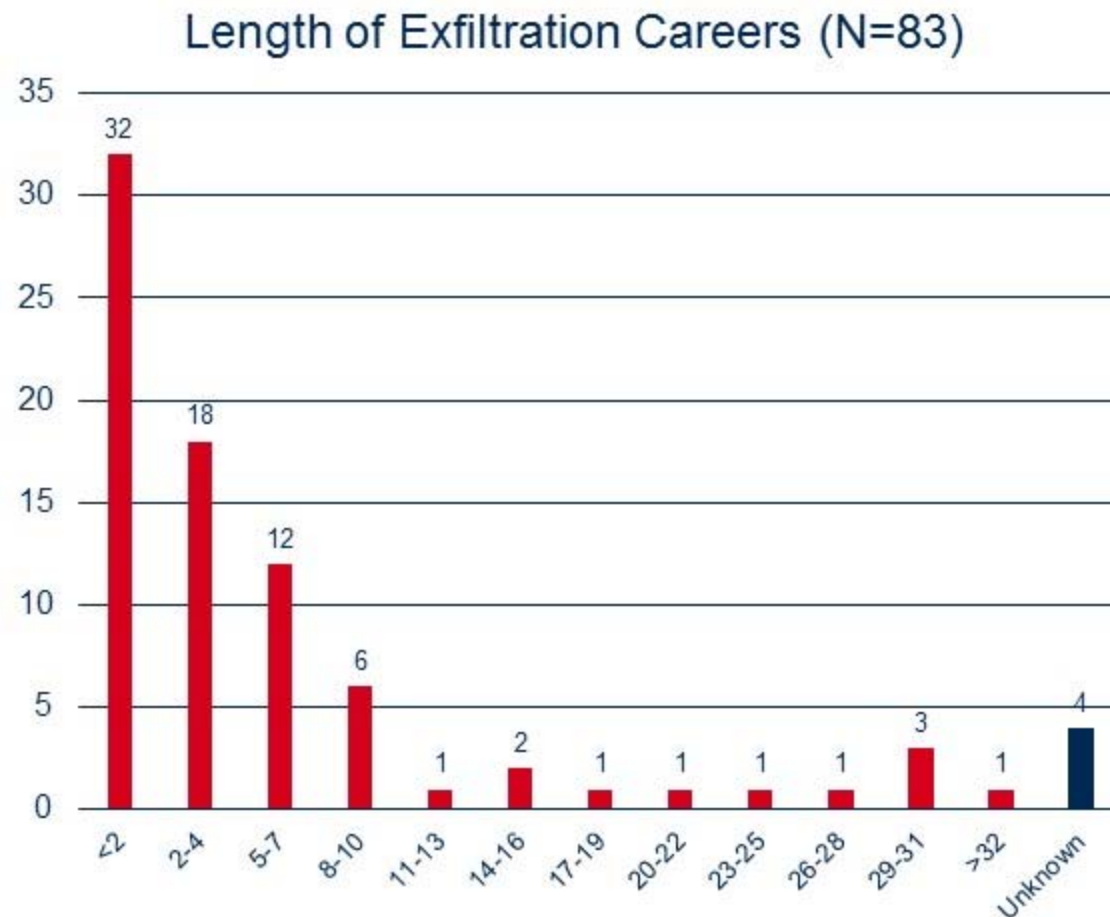
Highest Classification of Exfiltrated Material
(N=83)



Of the 56 cases for which relevant open source intelligence was available:

- 6 perpetrators exfiltrated only unclassified resources
- 50 perpetrators exfiltrated classified resources
 - 21 Classified (Level Unknown)
 - 16 Secret
 - 10 Top Secret
 - 3 SCI

RESULTS: THE WHEN



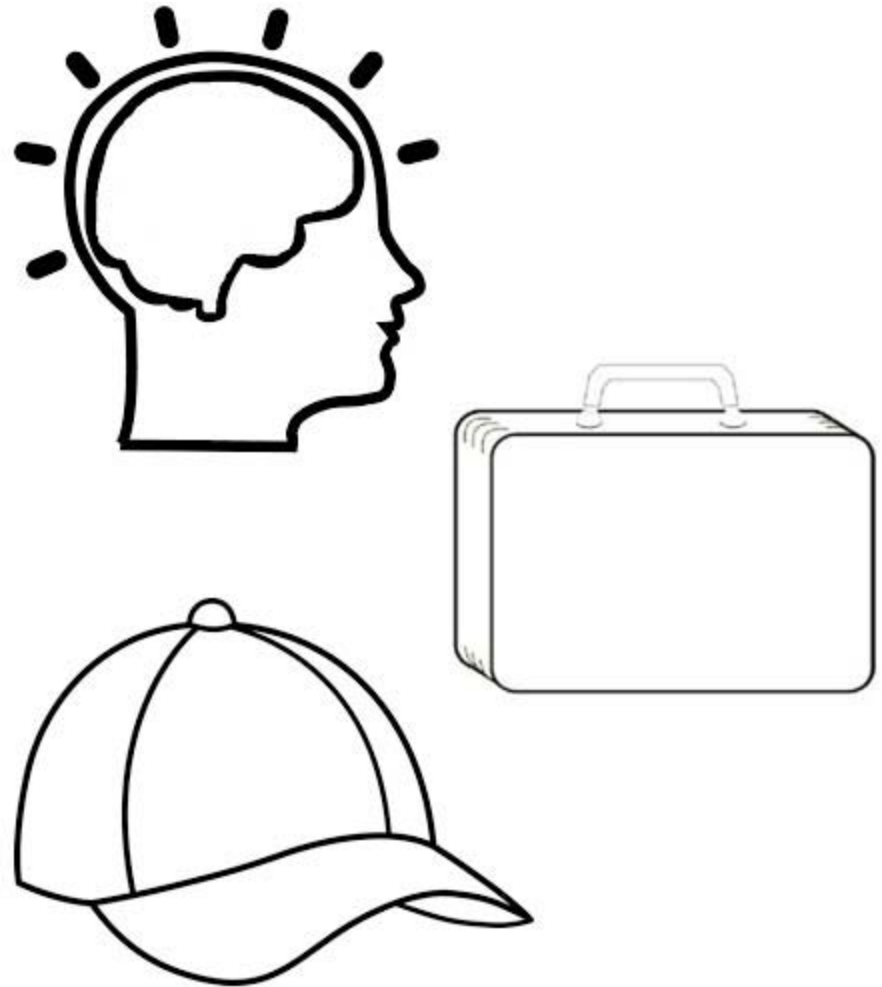
Of the 79 perpetrators for whom relevant open source intelligence was available:

- 32 perpetrators were active for less than 2 years
- 5 perpetrators were active for more than 25 years
- Of the four women included in this study, two had exfiltration careers that lasted longer than 10 years

RESULTS: THE HOW

Of the 37 cases for which relevant open source intelligence was available:

- 17 perpetrators concealed resources in a container of some kind, usually a briefcase or bag
- 7 perpetrators concealed resources on themselves (e.g., pocket, under hat)
- 10 perpetrators exfiltrated resources via email or fax
- 4 perpetrators misused courier card privileges
- 11 perpetrators never physically exfiltrated anything/worked from memory



RESULTS: THE WHY

Divided Loyalty

Ideology

Honeytrap **Revenge**

Ingratiation Blackmail

Money Career

Excitement

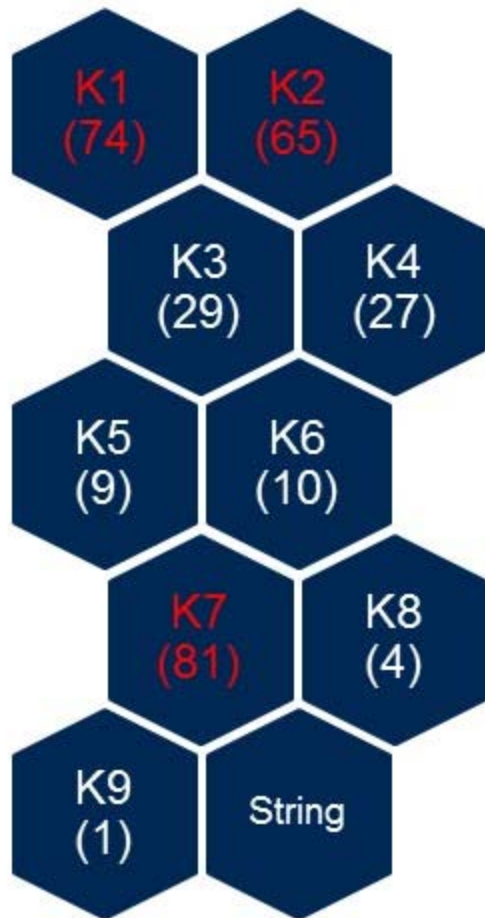


RESULTS: ADJUDICATIVE GUIDELINES

Perpetrators' Pre-Arrest Behaviors Categorized by Adjudicative Guideline



RESULTS: ADJUDICATIVE GUIDELINES



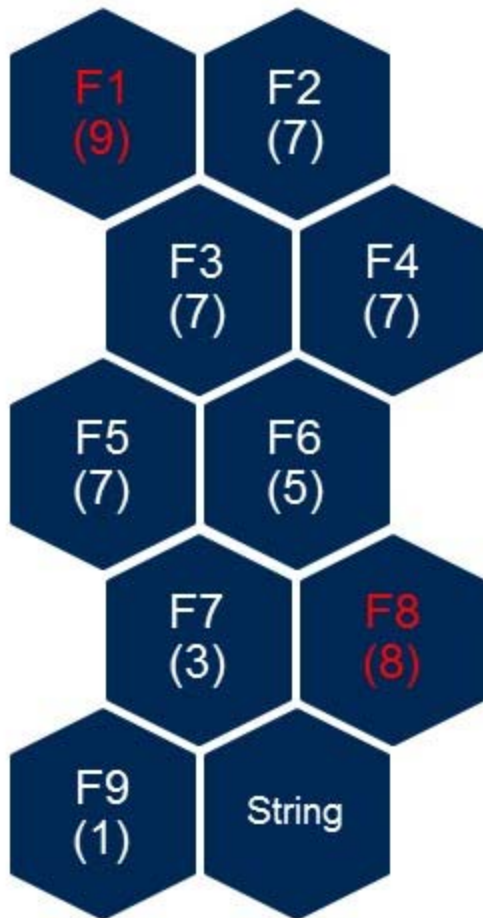
Guideline K:
Handling Protected Information

K1: “Person engaged in deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including, but not limited to, personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences.”

K7: “Person failed to comply with rules for the protection of classified or other protected information.”

K2: “Person collected or stored classified or other protected information at home or in any other unauthorized location.”

RESULTS: ADJUDICATIVE GUIDELINES



Guideline F:
Financial Considerations

F1: "Person demonstrated an inability or unwillingness to satisfy debts."

F8: "Person demonstrated unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that could not be explained by known legal sources of income."

RESULTS: BEHAVIORAL THREAT ASSESSMENT

CONCERNING COMMUNICATIONS

- Prior to arrest, 21 perpetrators talked about their exfiltration activity to at least one other person who was not an accomplice, a handler, or someone posing as a handler
 - 10 talked with friends
 - 9 talked with professional colleagues
 - 3 talked with family members
 - 3 talked with online acquaintances

Total exceeds 21 because some perpetrators talked with multiple people

CONCERNED OTHERS

- In 32 cases, someone noticed perpetrator's concerning behavior or a change in behavior prior to arrest
 - In 23 cases, someone reported perpetrator's concerning behavior or a change in behavior prior to arrest

FINDINGS

- Finding #1: Other than being male, there is no demographic profile of an employee who is likely to exfiltrate DoD resources
- Finding #2: User activity monitoring enables DoD to observe the electronic movement of its resources, but there appears to be insufficient protections against unauthorized physical movement
- Finding #3: The Adjudicative Guidelines are limited as a source for empirically-informed, pre-arrest behavioral indicators
- Finding #4: Behavioral threat assessment categories normally applied to violent crimes have the potential to inform pathways to non-violent crimes



OPA
OFFICE OF PEOPLE ANALYTICS

PERSEREC
DEFENSE PERSONNEL AND SECURITY RESEARCH CENTER

For More Information or to Request a Copy of the Final Report

Stephanie L. Jaros

Project Director

Stephanie.L.Jaros.civ@mail.mil

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-fiancé. 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/responder 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



CDSE Center for Development of Security Excellence

Insider Threat Training POC:

Rebecca Morgan

(410) 689-1294

Email: Rebecca.a.morgan22.civ@mail.mil



CDSE

Center for Development
of Security Excellence