CDSE Center for Development of Security Excellence

COUNTERINTELLIGENCE TRAINING AND AWARENESS CURRICULUM OVERVIEW

Thomas C. Gentle
CI Curriculum Manager

LEARN. PERFORM. PROTECT.

Mission & Vision

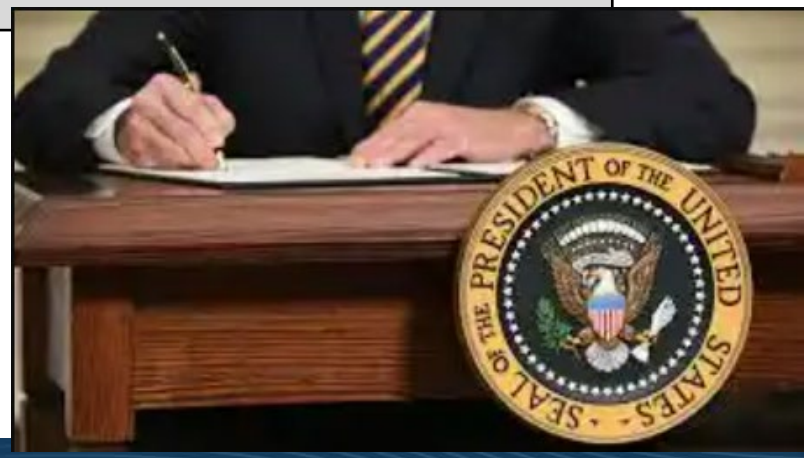
The Counterintelligence (CI) Awareness Program's purpose is to:

- Enhance DOD and Industry Security personnel awareness of their responsibility to report unusual activities and behaviors.
- Drive understanding of current threats from Foreign Intelligence Entities (FIE), other illicit collectors of US defense information, and terrorists.
- Educate and empower new and current counterintelligence professionals
  - Standardization and enhancement of products and services including Instructor Lead Training (ILT), Virtual Instructor Lead Training (VILT) and Mobile Training

Counterintelligence Defined

Executive Order (E.O.) 12333 (amended) Intelligence Activities:

Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.



The Role of Counterintelligence

Counterintelligence is real-time threat awareness, which helps to:

- Identify threats to your facility or operations
- Focus security efforts
- Deter foreign intelligence collection efforts
- Use threat-appropriate countermeasures
- Potentially save resources on security

Foreign Collectors

Who is targeting facilities?

Illicit collectors of U.S. information includes:

- Individuals
- Insider Threats (InT)
- Foreign Intelligence Entities (FIE)
- Quasi-Governmental Entities
- Commercial Enterprises

Targets of Foreign Collection

Both classified and unclassified information & technology are targets.

Targeted information includes:

- Sensitive company documents
- Proprietary information
- Export controlled/classified information and technology
- Information on DOD-funded contracts
- Dual-use technology
- Military critical technology

Reporting and Consequences

Title	Policy #	Notes
National Industrial Security Program Operating Manual (NISPOM)	32 CFR Part 117	• Suspicious contacts, adverse information • SEAD 3 (Foreign Travel, Foreign Contacts) • Actual espionage, sabotage, terrorism, subversive activity to FBI • 32 CFR Part 117 NISPOM Rule (dcsa.mil)
Counterintelligence Awareness and Reporting (CIAR)	DODD 5240.06	• Identify and Report: Foreign Collection Activities; Foreign Cyber Activities; Potential Espionage Indicators; Insider Threat; Anomalous Health Inci • d5240_06.pdf (menlosecurity.com)

****Civilian personnel: Disciplinary action under regulations governing civilian employees****

Reporting and Consequences

Title	Policy #	Notes
Intelligence Oversight	DODD 5148.13	• Questionable Intelligence Activities (QIA) • Significant/Highly Sensitive Matter (S/HSM) • Intelligence or related activity reportable to the U.S. Attorney General • DoD Directive 5148.13, April 26, 2017 (defense.gov)
Uniform Code of Military Justice (UCMJ)	Article 92	• Military: Failure to report may result in UCMJ action (failure to obey order or regulation) • Arts9293Jun15.pdf (defense.gov)

Civilian personnel: Disciplinary action under regulations governing civilian employees

What are some of the Counterintelligence Policies?

- DODD 5240.02 Counterintelligence
- DODD 5240.06 Counterintelligence Awareness and Reporting
- DODD 5148.13 Intelligence Oversight Awareness
- NISPOM 32 CFR Part 117

Our CDSE Instructors, Audience, and Stakeholders

- Subject Matter Experts (SMEs) with years of experience in the military and U.S. Government
- DOD Counterintelligence Professionals
- DOD and Cleared Industry Professionals

Our Current Counterintelligence Curriculum Catalog

The Counterintelligence Curriculum catalog consists of a diverse range of CI training and awareness products. CI Instructors also provide CI instructor-led training (ILT) within other security disciplines.

- CI Presentations with instructor-led training (in-person and virtual)
- 11 eLearning courses
- 1 Toolkit
- 11 Security Shorts
- 10 Job Aids
- 21 Webinars
- 40 CI-Related Case Studies (see Case Study Library)
- 2 Games
- 8 Posters

Future Curriculum Goals

- Pioneer innovative products
- Strengthen awareness messaging for a diverse audience
- Strengthen and broaden collaborative relationships with stakeholders and professionalization partners
- Improve standing as a leader of counterintelligence training
- Contribute to training and awareness strategy
- Optimally incorporate DOD CI policy changes into training and awareness curriculum

GFY25 Counterintelligence Curriculum Content

Content Themes:

- Artificial Intelligence
- Behavioral Science
- Fraud

- 1 eLearning (Fraud and CI Content)
- 2 Security Shorts (AI and Personal Vetting and CI Content)
- 4 Job Aids (CI and Vetting Content)
- 5 Webinars (incl. Supply Chain, AI, and Fraud Content)
- 40 CI-Related Case Studies (see Case Study Library)
- 2 Videos (Profile in Espionage and Targeting by Adversaries)
- 5 Posters (incl. Behavioral Science, Fraud, and Supply Chain)

Upcoming CDSE, DCSA CI Webinars

- 21 Nov 2024 – Topic TBD
- 20 Feb 2025 – Topic TBD (Perhaps Supply Chain Related)
- 15 May 2025 – Topic (Perhaps AI Related)
- 17 July 2025 - Topic TBD
- 18 Sep 2025 – Fraud and CI Risks

Register at https://www.cdse.edu/Training/Webinars-and-Conferences

CDSE Center for Development of Security Excellence

INSIDER THREAT TRAINING AND AWARENESS CURRICULUM OVERVIEW

Amber D. Jackson
Insider Threat
Curriculum Manager

LEARN. PERFORM. PROTECT.

Mission & Vision

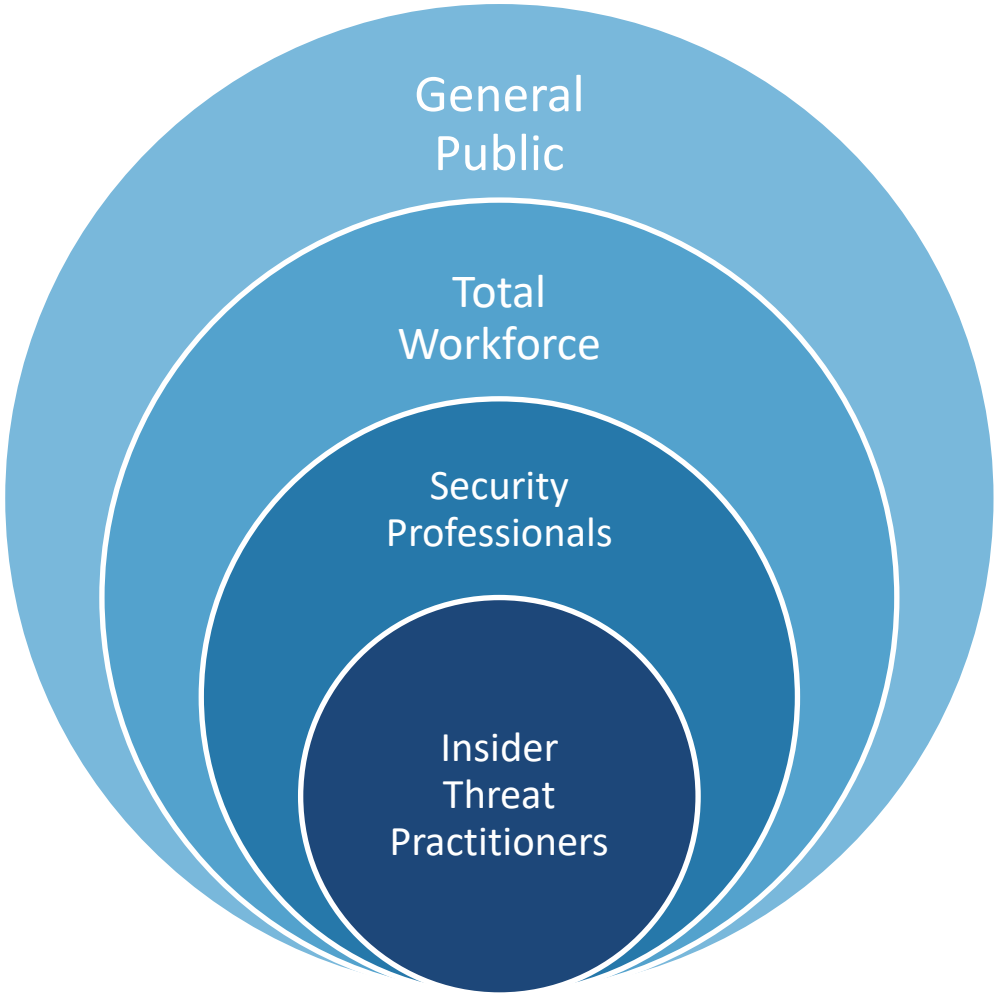
Awareness

Training

Professionalization Support

Public Outreach

Our Audience



- Outreach
- Awareness
- Training
- Professionalization

Insider Threat Defined

The 2017 National Defense Authorization Act defines an insider threat for the Department of Defense as, “a threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of the Department and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or a destructive act, which may include physical harm to another in the workplace.”

The Role of Insider Threat Programs

- Designed to deter, detect, and mitigate actions by insiders who may pose a threat to their organization.
- Employ holistic and multidisciplinary responses when managing insiders who are at risk, while maintaining their privacy and civil liberties.
- Do not conduct investigations

What are some of the Insider Threat Policies?

- Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011

- Presidential Memorandum, National Insider Threat Policy & Minimum Standards for Executive Branch Insider Threat Programs, November 11, 2012

- DODD 5205.16, The DOD Insider Threat Program, Change 2, September 9, 2017

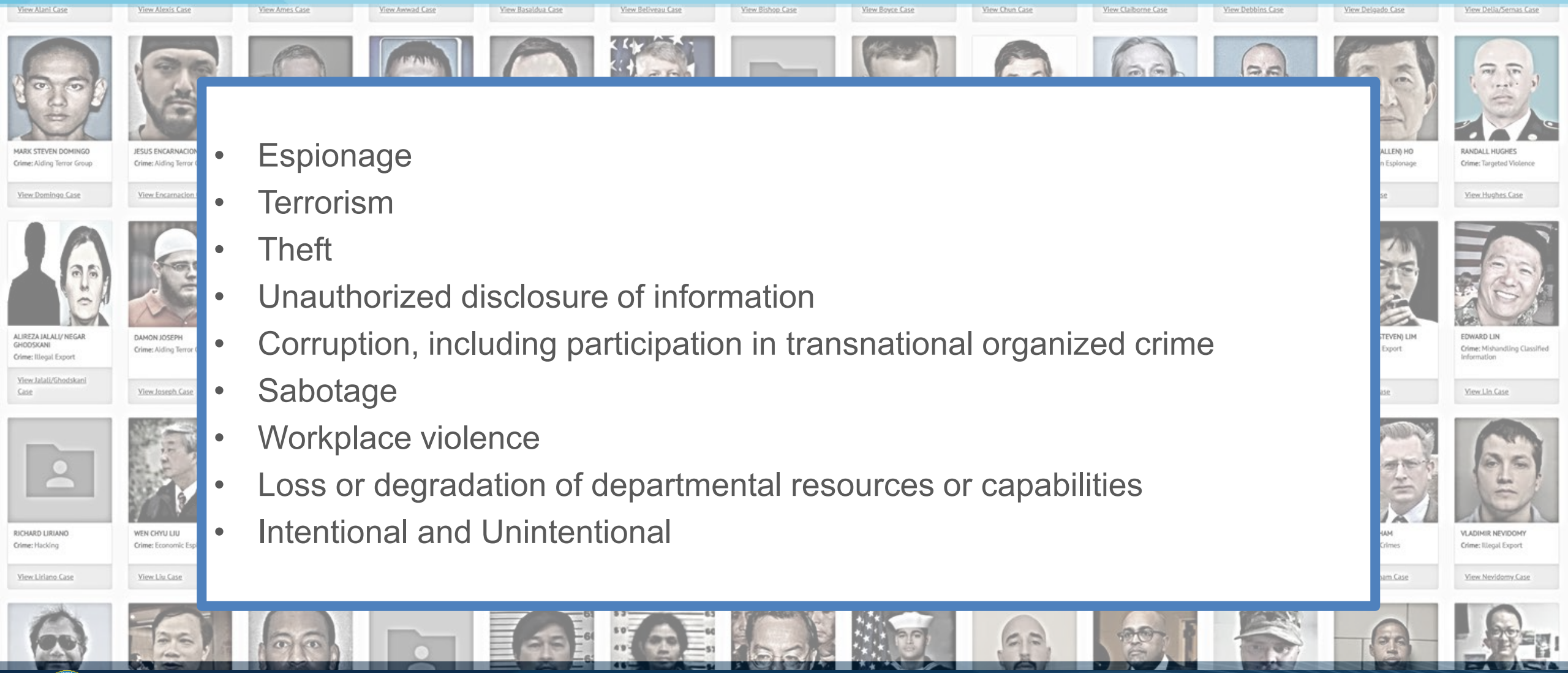
- 32 CFR Part 117, “National Industrial Security Program Operating Manual (NISPOM)”, February 24, 2021

Poll Question #1

Which policy is about to be reissued/updated?

- Presidential Memorandum, National Insider Threat Policy & Minimum Standards for Executive Branch Insider Threat Programs, November 11, 2012
- DODD 5205.16, The DOD Insider Threat Program, Change 2, September 9, 2017
- 32 CFR Part 117, “National Industrial Security Program Operating Manual (NISPOM)”, February 24, 2021

Insider Threat Landscape



- Espionage
- Terrorism
- Theft
- Unauthorized disclosure of information
- Corruption, including participation in transnational organized crime
- Sabotage
- Workplace violence
- Loss or degradation of departmental resources or capabilities
- Intentional and Unintentional

Current Catalog

≈300 Products and Resources

2	12	50+	1	36	75+
CURRICULA	ELEARNINGS	WEBINARS	VIRTUAL INSTRUCTOR-LED TRAINING	VIDEOS	CASE STUDIES
10	50+	1	50+	4	13
GAMES	POSTERS	SECURITY CAMPAIGN WEBSITE	JOB AIDS	SECURITY SHORTS	TOOLKIT TABS

Upcoming ITDAC Iterations (GFY2025)

Registration Checklist

- ✓ Complete INT311.CU or INT312.CU
- ✓ Eligibility Form
  - Provide Supervisor Information
  - CTR Provide Government Lead
  - Provide Direct Support to USG Insider Threat Programs, Role Supports Hub Component

OCT | 21-25, 2024	APR | 7-11, 2025
NOV |18-22, 2024	MAY |12-16, 2025
DEC | 2-6, 2024	JUN | 23-27, 2025
JAN |13-17, 2025	JUL | 21-25, 2025
FEB |10-14, 2025	AUG | 18-22, 2025
MAR |17-21, 2025	SEP | 22-26, 2025

Shorts

This interactive story demonstrates the importance of cultural competence when managing risk in a cross-cultural setting and encourages reporting of concerning behavior to the Insider Threat Program.

Enhance understanding of the interconnected, multi-disciplinary approach used by insider threat programs to collect multiple data points from divergent sources and to combine them in ways that regard the “whole person” when detecting and assessing potential risk.

Webinars

- An Alternative View of Preventing Insider Threats
- Understanding and Leveraging the Role of Law Enforcement and Counterintelligence
- Online Behavior in Threat Assessment
- Stalking Fundamentals
- Extremism: An Overview from the Department of Justice
- Saying Goodbye: Making Involuntary Separations Easier and Safer
- Mass Shooter Contagion Theory and The Copycat Effect in the Evolving Media Environment

BTAC Bulletin

A monthly publication, highlights emerging threats, trends, capabilities, and best practices to increase awareness across the DOD insider threat enterprise. Content will focus on training, reference material and other resources relevant to leaders and insider threat professionals.

- Building Positive Culture
- Moral Outrage
- Psychological Risk Factors
- "Red Flag" Laws
- Sexual Violence
- Unauthorized Disclosure

AUGUST 2024

ORIGINS OF RADICALIZATION

BTAC BULLETIN

BEHAVIORAL SCIENCE | LAW ENFORCEMENT & COUNTERINTELLIGENCE | CYBERSECURITY | EMPLOYEE MANAGEMENT RELATIONS | THREAT ASSESSMENT & MANAGEMENT

ORIGINS OF RADICALIZATION

IDENTITY, NEEDS, & SOCIAL NETWORKS

There is no one pathway of radicalization; it involves many psychological, cultural, and social factors by which individuals become increasingly accepting of violence for a cause. Those who turn to violent extremist behavior rarely do so out of a simple desire for violence, but instead because they are attempting to address unmet NEEDs and they have come to view the world through a NARRATIVE of personal grievance that has been reinforced by a NETWORK of like-minded people[1]. This dynamic and multi-faceted process is influenced by personal biopsychosocial factors (psychological vulnerabilities and personality traits) and Push/Pull factors in their environment[2,3]. *Push factors* are real or perceived situational influences that drive the individual toward radicalization like a personal grievance, while *Pull factors* are group-level factors involving the network and environmental context that draw the individual to seek information, experiences, and other individuals that align with their newly developing ideology, reinforcing their grievance narrative.

PUSH → PULL → RADICALIZATION

IDENTITY CHALLENGE	NEEDS	NARRATIVE	NETWORK	NEW MORAL IDENTITY	MORAL OUTRAGE
Unexpected or impactful life events can cause people to radically change how they view themselves and the world around them. This can lead to challenges to identity and a reappraisal of their values and needs.	A primary component of radicalization is an origin in unmet universal NEEDS; Needs for food, safety, housing, appreciation, and belonging.	The NARRATIVE is the story an individual uses to structure meaning related to a grievance, that can be hijacked by an extremist social network towards a particular ideology.	The NETWORK, is the culture or social group that provides a sense of belonging and helps an individual develop a shared narrative that encourages extreme action.	Together, the needs, narrative, and network guide an individual toward a NEW MORAL IDENTITY, by emphasizing a new interpretation of values and beliefs that can push and pull a person further down the pathway to violence.	A network may attempt to leverage this new moral identity to direct MORAL OUTRAGE at a newly developed or magnified grievance through violence.

3N's MODEL[1]

MORAL IDENTITY & HUMAN NEEDS

When someone experiences a crisis of identity brought on by significant life change (e.g., employment loss, separation from service, relationship change, moral injury, or relocation) they can experience emotional upheaval that renders them more vulnerable to violent radicalization. Individuals faced with an identity challenge seek to make sense of their experiences and fulfill newly unmet needs. While many support groups are protective and helpful, violent extremist groups take advantage of these needs by filling voids and providing supportive camaraderie, shared backgrounds, and ultimately a shared grievance narrative.

Violent extremist groups can provide a social network and narrative through which a person can interpret their recently experienced turmoil. Consider an individual isolated in a new foreign environment not knowing the language and without money, or a person who has been terminated from a position in career they have strongly identified with. Without support, and under the right circumstances, violent extremist groups can take advantage of these individuals and provide or reinforce a narrative of hate and anger which may move them further down the extremism spectrum, pushing and pulling them toward radicalization and criminal behavior.

MITIGATION STRATEGIES

- Develop and communicate local work conduct guidelines that define extremist behavior, and follow-up on all reports of potential radicalization indicators. Early action may reduce the risk of behaviors escalating to violence.
- Promote social engagement and encourage participation in community organizations and activities that support positive identity development.
- Proactively manage separations by providing resources. (e.g., health care, resume updates, career counseling) and encourage language that implies continued connection and belonging.

1. Webber, D., & Kruglanski, A. W. (2017). Psychological factors in radicalization: A "3N" approach. In The handbook of criminology of terrorism, 1st ed. G. LaFree & J.D. Freilich (Eds.), John Wiley and Sons. 2. Gill, P. (2012). "Terrorist violence and the contextual, facilitative and causal qualities of group-based behaviors." *Aggression and Violent Behavior*, 17, 565–574.

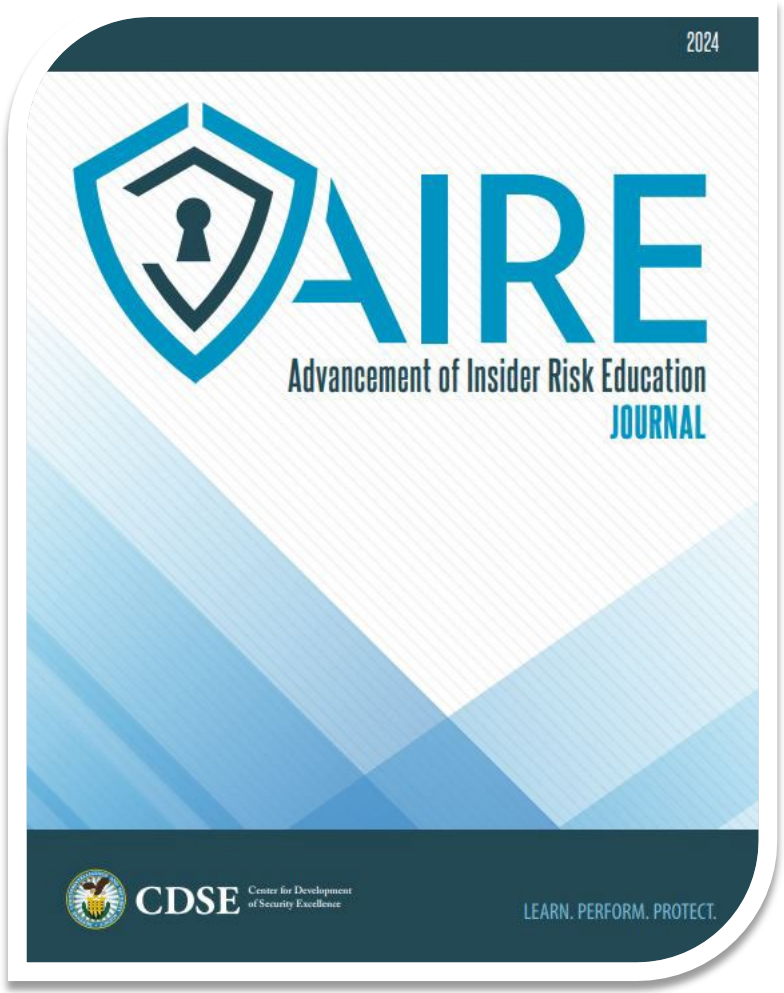
3. Morgan, J. (2005). *The psychology of terrorism*. London, United Kingdom: Routledge. 4. Institute for Defense Analyses (2023). *Prohibited Extremist Activities in the U.S. Department of Defense*.

DITMAC DOD Insider Threat Management and Analysis Center

Behavioral Threat Analysis Center (BTAC) // A Multidisciplinary Team

E-Mail/Sign Up For The Bulletin: dcsa.quantico.dcsa.list.ditmac-smo@mail.mil

Advancement of Insider Risk Education (AIRE) Journal



IN THIS ISSUE

What the CDSE Can Offer You 1

Highlighted Training Products 4
eLearning INT101: Insider Threat Awareness 5
DCSA Counter-Insider Threat Community Training Series 8
Insider Threat Detection Analysis Course 9

Top Five Trends For Training Development 11

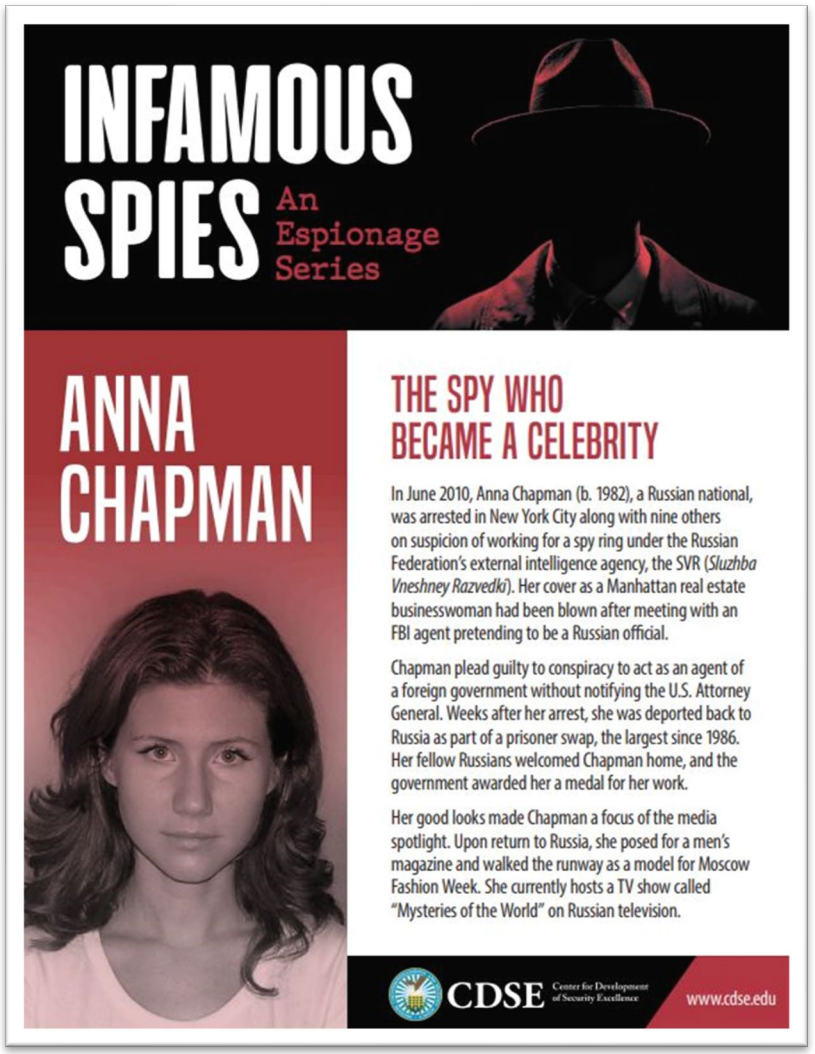
Highlighted Education Products 16
ED 520: Foundations of Insider Threat Management 17

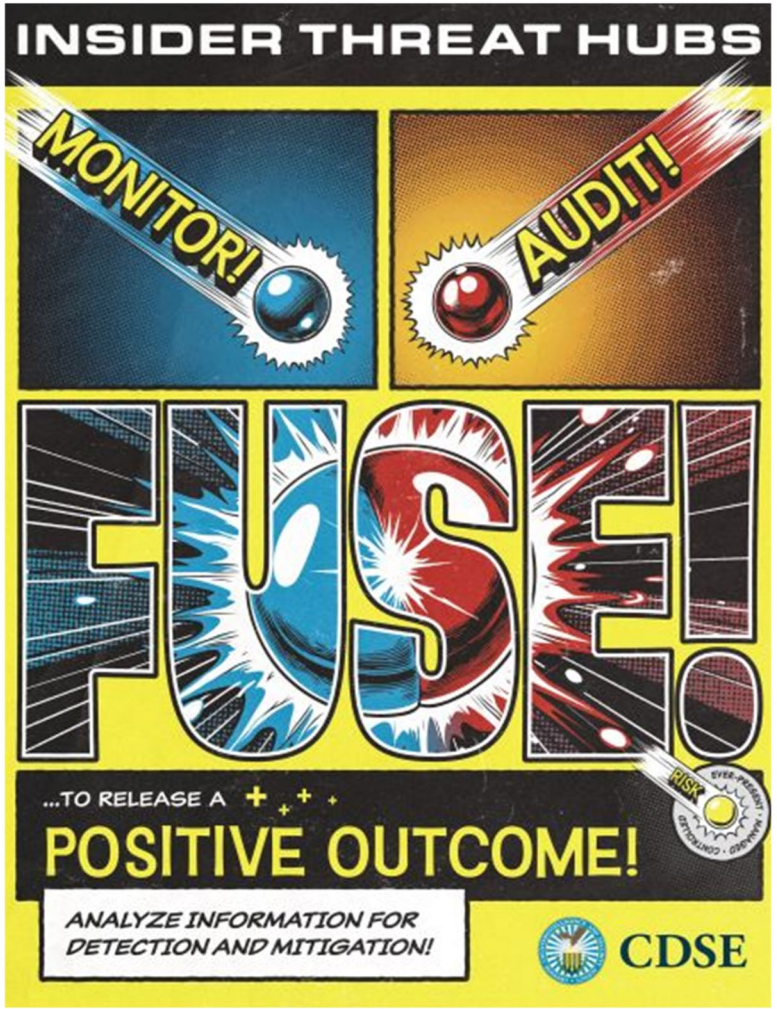
A Strategy for Professionalization 19

Highlighted Certification Products 24
Certified Credible: Counter-Insider Threat Professionals Get Their Own Exam 25
Certified Counter-Insider Threat Professional (CCITP) Certification 27

Helpful Tools 30
Insider Threat Program Operations Personnel Requirements 31
Hub Analyst Training Roadmap 33
Directory of Resources 47
About DCSA 49
CDSE Contact List 50

Posters

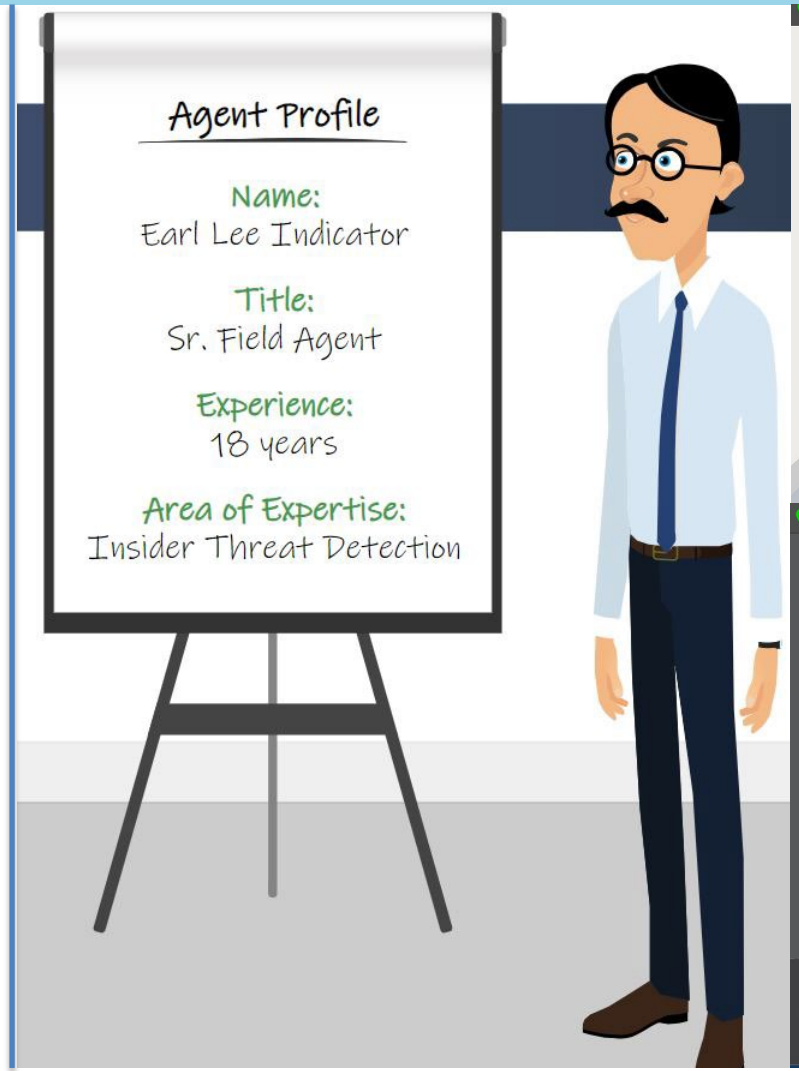

INFAMOUS SPIES
An Espionage Series
ANNA CHAPMAN
THE SPY WHO BECAME A CELEBRITY
In June 2010, Anna Chapman (b. 1982), a Russian national, was arrested in New York City along with nine others on suspicion of working for a spy ring under the Russian Federation's external intelligence agency, the SVR (Sluzhba Vneshney Razvedki). Her cover as a Manhattan real estate businesswoman had been blown after meeting with an FBI agent pretending to be a Russian official.
Chapman plead guilty to conspiracy to act as an agent of a foreign government without notifying the U.S. Attorney General. Weeks after her arrest, she was deported back to Russia as part of a prisoner swap, the largest since 1986. Her fellow Russians welcomed Chapman home, and the government awarded her a medal for her work.
Her good looks made Chapman a focus of the media spotlight. Upon return to Russia, she posed for a men's magazine and walked the runway as a model for Moscow Fashion Week. She currently hosts a TV show called "Mysteries of the World" on Russian television.
CDSE Center for Development of Security Excellence
www.cdse.edu

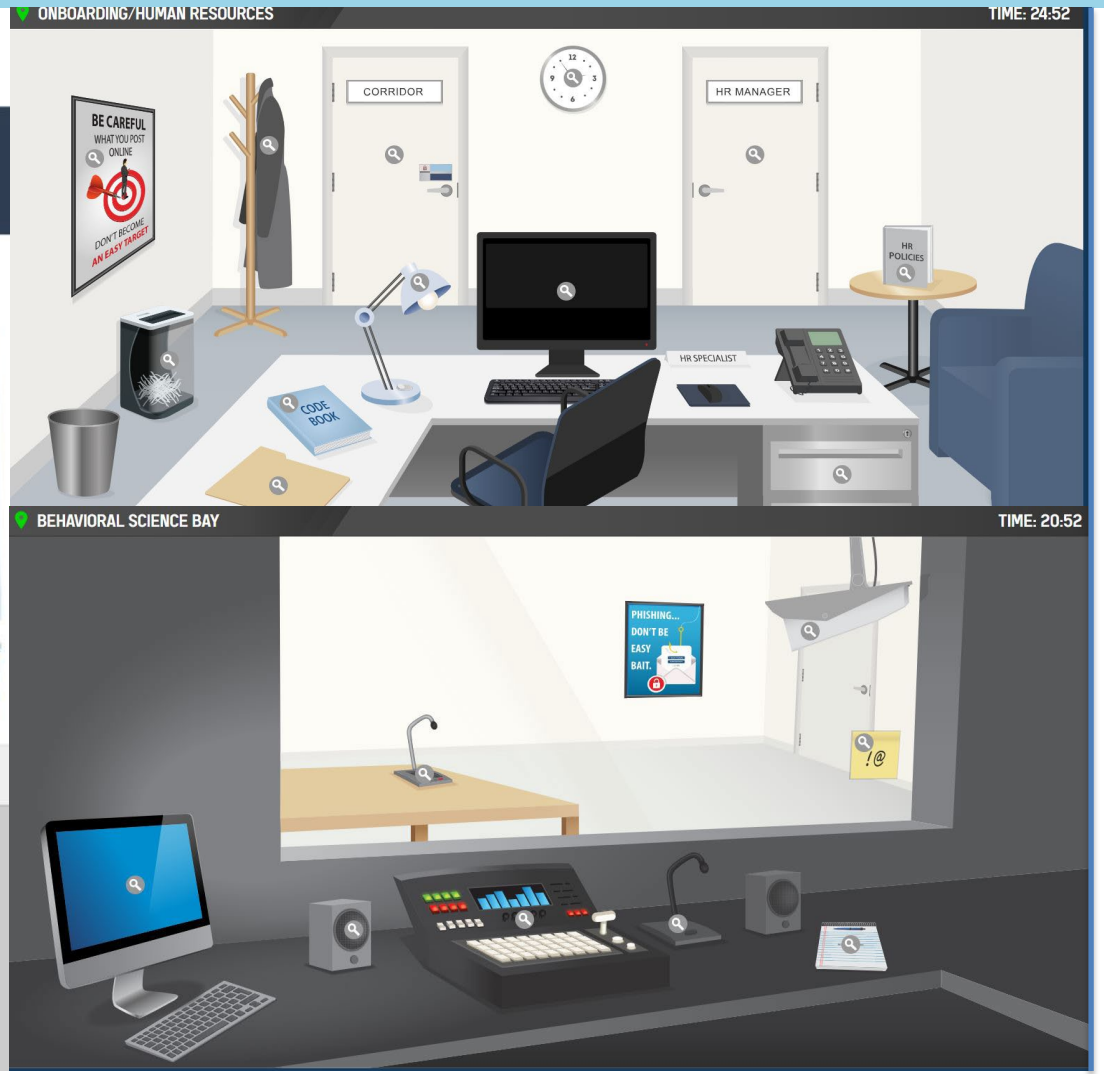

INSIDER THREAT HUBS
MONITOR!
AUDIT!
FUSE!
...TO RELEASE A
POSITIVE OUTCOME!
ANALYZE INFORMATION FOR DETECTION AND MITIGATION!
CDSE

SPARK THE CONVERSATION
Victims of malicious insider acts are our family and friends.
Learn to recognize indicators of an insider threat.
Raise awareness.
CDSE Center for Development of Security Excellence
NITAM
September is National Insider Threat Awareness Month

Games

- Trivia Twirl
- Concentration
- Whodunnit
- Who is the Risk?
- Crossword Puzzles
- Word Search
- Escape Rooms

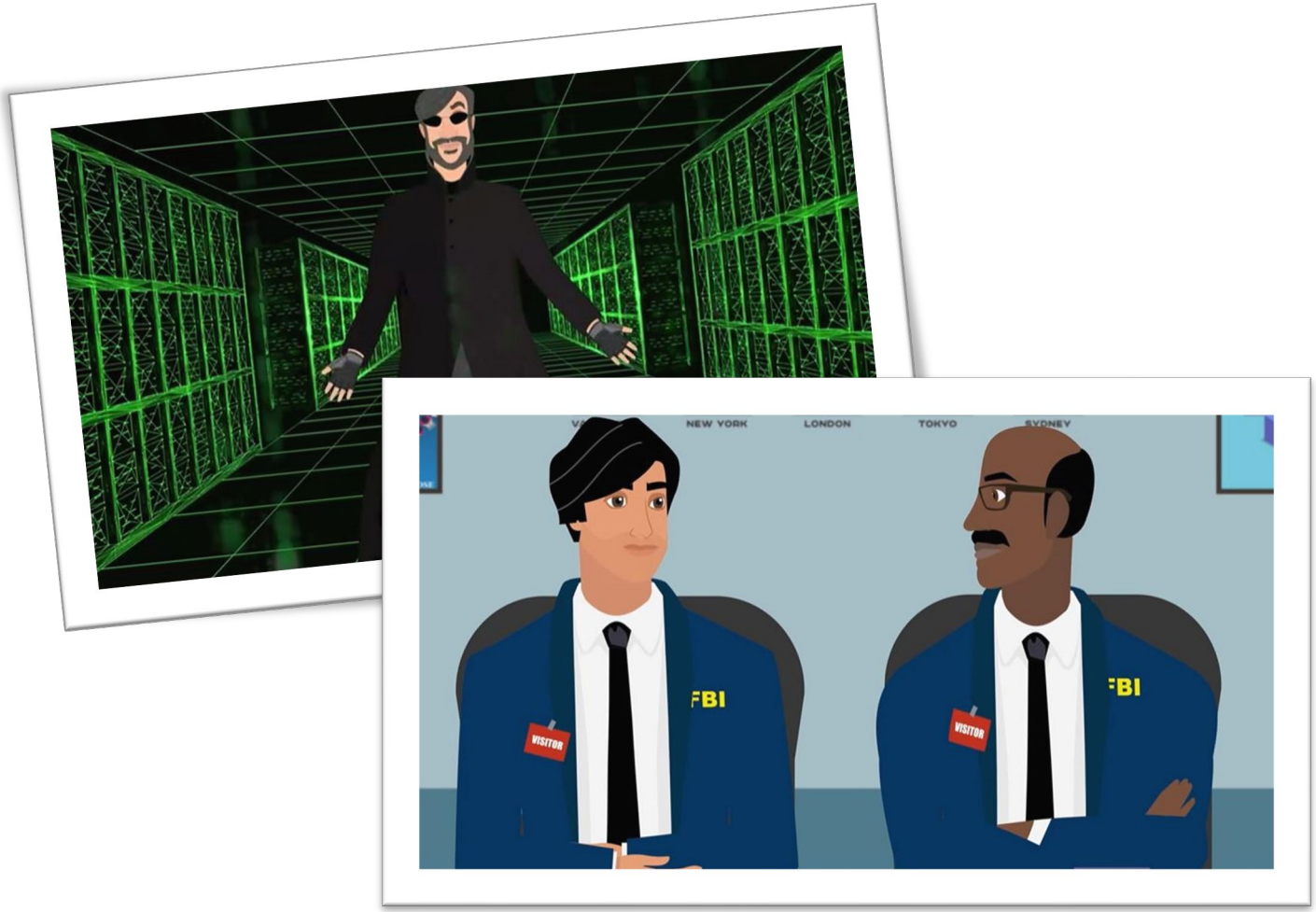




Poll Question #2

- Have you played The Adventures of Earl Lee Indicator?
- Yes
- No

Witting and Unwitting



In the animated series, executive Marc Connors is overlooked for a promotion that goes to a colleague instead. Frustrated and disgruntled, Marc begins disrupting corporate operations to retaliate for his perceived rejection and cause as much damage to the company as he can, in secrecy.

Episode 1: Overlooked

Episode 2: Hacked

Episode 3: Unexpected Capacity

Episode 4 – Winter 2024

Insider Threat Vigilance Videos

The Insider Threat Vigilance Video Series aids the workforce in identifying and reporting insider threat indicators.

Season 1: *Turning People Around, Not Turning Them In*
(four episodes)

Season 2: *The Critical Pathway*
(four episodes)

Season 3: *Honor in Hindsight*
(four episodes)

National Insider Threat Awareness Month

September 26, 2024 | HQMC Marine Corps Virtual Workshop #5: **"Should the Insider Threat/Risk Community Be Concerned about Online Gaming“** : Participants will be provided an overview on online gaming as an emerging threat/risk. The topic is relevant and timely considering the recent high-profile incident involving disclosure of classified information on a gaming platform.

Poll Question #3

- Did your organization host an event or share resources for NITAM?
- Yes
- No

On the Horizon

- Tabletop Exercise (asynchronous activity)
- Updates to Insider Threat Detection Analysis Course
- New Offerings DCSA Counter Insider Threat Training Series
- Case Studies
- Job Aids
- Updates to eLearnings
- New eLearning for Supervisors and Commanders
- Awareness Videos
- Supplemental Virtual Instructor-Led Training
- AIRE – 2nd Issue

Resources

- AIRE: https://securityawareness.dcsa.mil/aire.html
- Archived Webinars: https://www.cdse.edu/Training/Webinars-and-Conferences/
- BTAC Bulletin: https://www.dcsa.mil/Counterintelligence-Insider-Threat/DITMAC/
- Case Study Library: https://securityawareness.dcsa.mil/cdse/case-studies/index.php
- Catalog: https://www.cdse.edu/Training/Insider-Threat/
- Games: https://www.cdse.edu/Training/Security-Awareness-Games/
- ITDAC Course Information: https://www.cdse.edu/Training/Virtual-Instructor-led-Courses/INT200/
- NITAM Website: https://securityawareness.dcsa.mil/cdse/nitam/index.html
- Posters: https://www.cdse.edu/Training/Security-Posters/Insider-Threat/
- Security Training Videos: https://www.cdse.edu/Training/Security-Training-Videos/Insider-Threat/
- Shorts: https://www.cdse.edu/Training/Security-Shorts/Insider-Threat-Security-Shorts/
- Upcoming Webinars: https://www.cdse.edu/Training/Webinars-and-Conferences/
- Witting and Unwitting:
  - E1 https://www.dvidshub.net/video/862223/cdse-witting-and-unwitting-overlooked
  - E2 https://www.dvidshub.net/video/885518/witting-and-unwitting-episode-2-hacked
  - E3 https://www.dvidshub.net/video/920651/witting-and-unwitting-unexpected-capacity

Contact Information

Please submit any questions or comments to the CDSE, DCSA training mailbox at:

dcsa.cdsetraining@mail.mil