



CDSE

Center for Development
of Security Excellence

Counterintelligence Webinar Series: The Venn of Counterespionage

LEARN.
PERFORM.
PROTECT.

TODAY'S SESSION

HOST:

Ed Kobeski, CDSE Counterintelligence

GUEST:

Ms. Rebecca Morgan



Attendee Participation & Feedback

Enlarge Screen



File Share



Closed
Captioning
below



Q & A



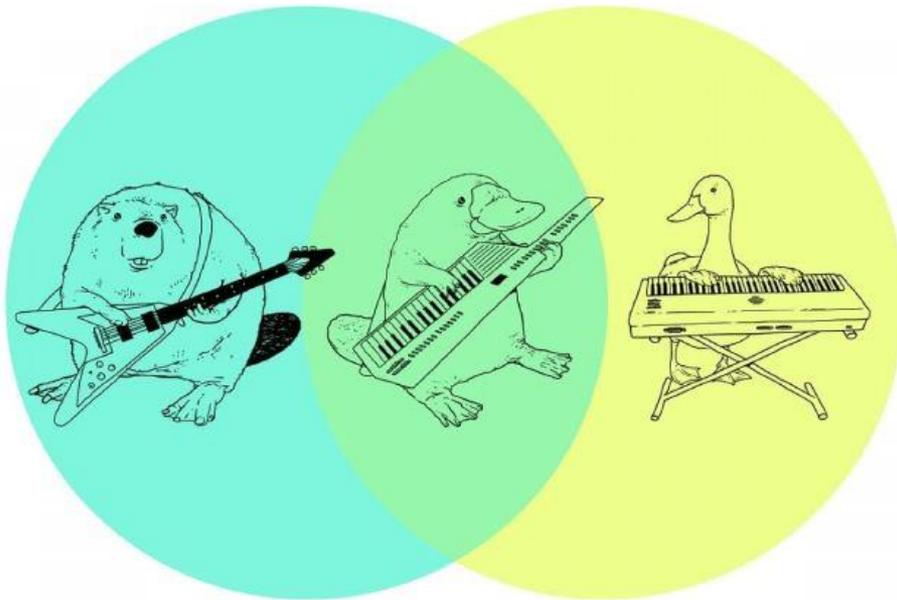
Agenda

- The Venn of Counterespionage
- CI Definitions
- Insider Threat Definitions
- The Divergence
- The Mergence
- Defense
- Lightning Round!

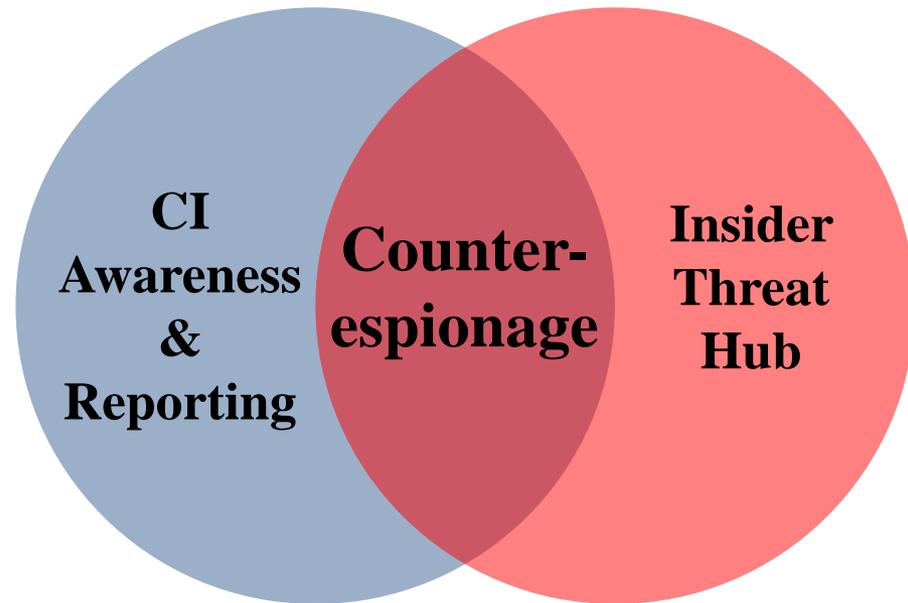


The Venn of Counterespionage

The greatest
Venn diagram ever



The ^{second} greatest
Venn diagram ever



Counterintelligence

- **Counterintelligence:** 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.
- **Counterespionage:** That aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities.



Insider Threat

- **Insider Threat (NISPOM DoD 5220.22-M):** The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.
- **Counterintelligence Insider Threat (CI InT):** A person, known or suspected, who uses their authorized access to DoD facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise DoD information, or commit espionage on behalf of an FIE (Foreign Intelligence Entity).
- **The Insider Threat Program:** A multidisciplinary capability designed to detect, deter and mitigate risk from an insider threat.



The Divergence

- **CI: Strictly Foreign intelligence Nexus**
- **CI examples generally NOT Insider Threat:**
 - Solicitation at a conference
 - Surveillance/ search seizures during foreign travel
 - Brute Force attack by APT1 against your network
- **Insider Threat examples generally NOT CI:**
 - Workplace Violence event
 - Unsafe practices due to drug/ alcohol abuse in work place

Legend

CI: Counterintelligence

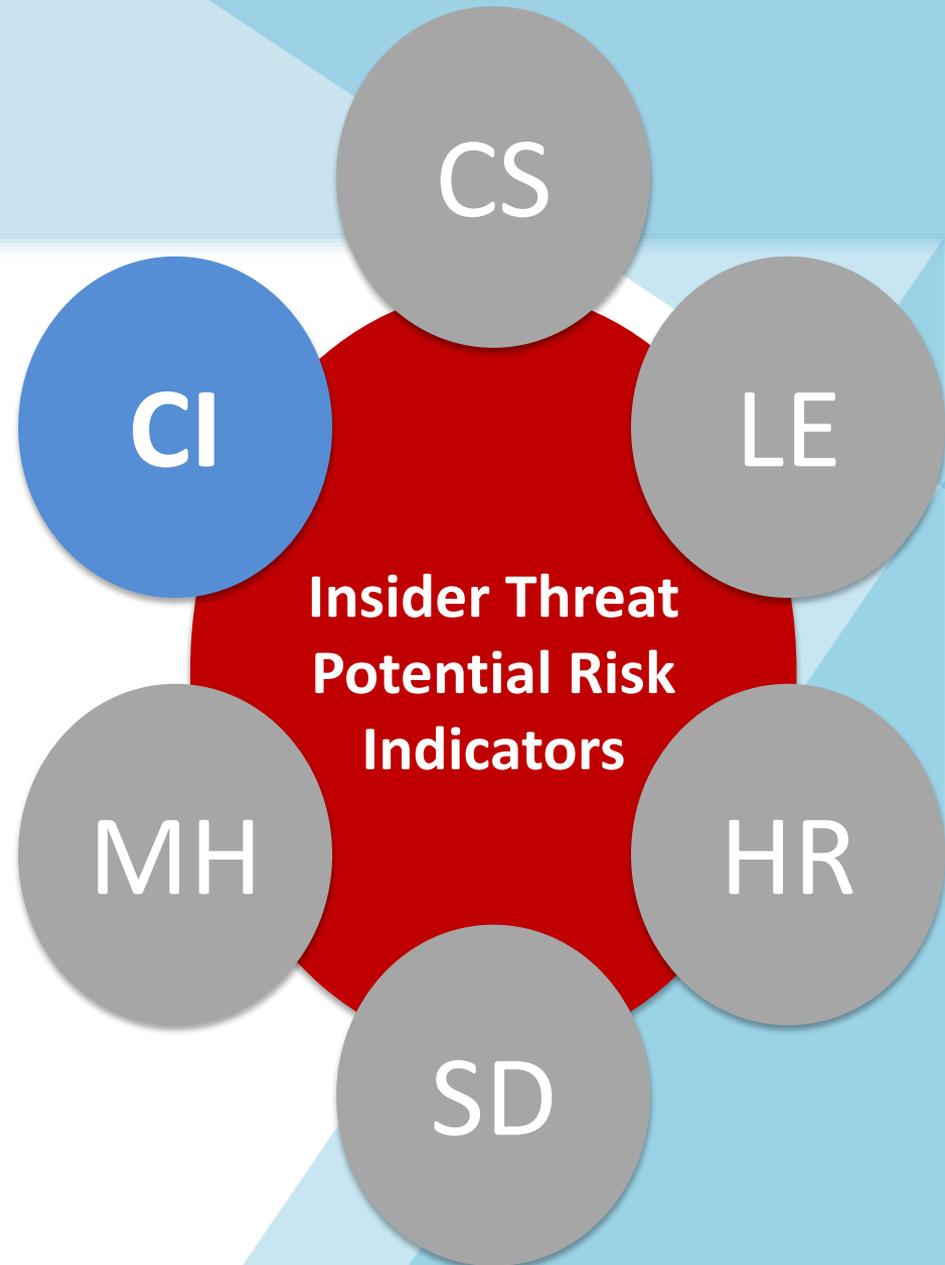
CS: Cyber Security

LE: Law Enforcement

HR: Human Resources

SD: Security Department

MH: Medical/ Mental Health



The ~~Mergence?~~ Convergence

- Supply chain, Foreign Intelligence Entities (FIE), insider enabled cyber, and poor security practices are areas of overlap
- Insider threat and CI convergence examples:
 - Employee clicking link to a malicious spear phishing email
 - Colluding with a competitor or foreign power
 - Surfing adult content on work computer
 - Knowingly or unknowingly purchasing sub-par or tampered with components

Legend

CI: Counterintelligence

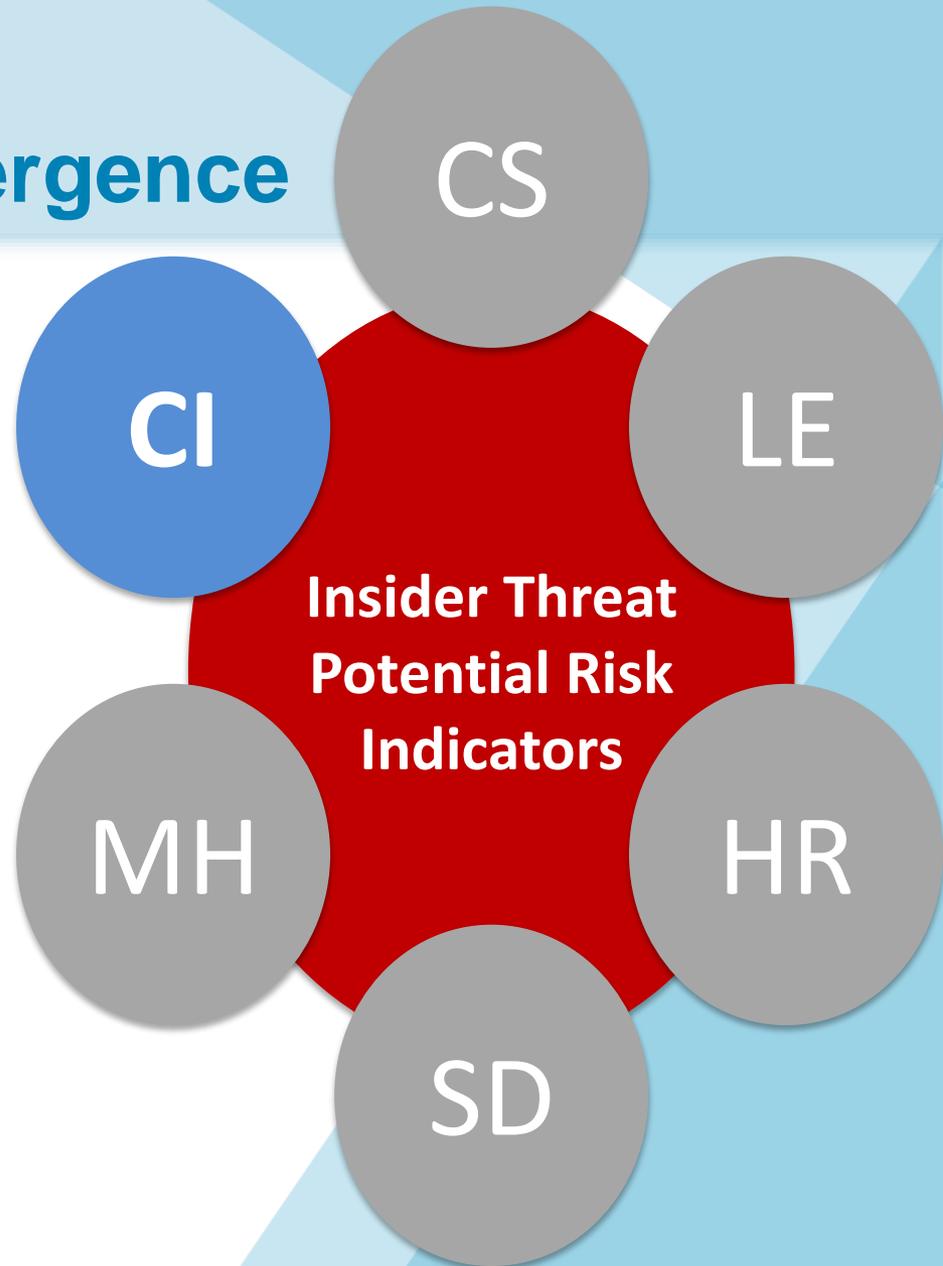
CS: Cyber Security

LE: Law Enforcement

HR: Human Resources

SD: Security Department

MH: Medical/ Mental Health



Defense!

Strategy	What can you do
Detect	<ul style="list-style-type: none">- Enhance awareness of the unintentional insider threat- Improve usability of security tools- Report- Continuously re-evaluate your security procedures
Deter	<ul style="list-style-type: none">- Training, Training, Training- Policies enforced
Deny	<ul style="list-style-type: none">- Provide effective security practices (e.g. two factor authentication for access)- Maintain staff values and attitudes that align with organizational mission and ethics
Mitigate	<ul style="list-style-type: none">- Insider Threat Programs can provide intervention for positive outcomes for individuals and organizations



Lightning Round! Question 1

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Someone clicks on a link or opens an attachment in a spear phishing email				



Lightning Round! Answer 1

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Someone clicks on a link or opens an attachment in a spear phishing email			X	



Lightning Round! Question 2

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
You find a tuft of cat fur in some muffins you bought at the bake sale				



Lightning Round! Answer 2

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
You find a tuft of cat fur in some muffins you bought at the bake sale				X



Lightning Round! Question 3

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
State sponsored CNE actor launches SQL attack on server				



Lightning Round! Answer 3

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
State sponsored CNE actor launches SQL attack on server	X			



Lightning Round! Question 4

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Disgruntled employee engages in work place violence				



Lightning Round! Answer 4

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Disgruntled employee engages in work place violence		X		



Lightning Round! Question 5

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Employee making suicidal gestures				



Lightning Round! Answer 5

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Employee making suicidal gestures		X		



Lightning Round! Question 6

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Reporting that you were surveilled at an overseas tradeshow				



Lightning Round! Answer 6

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Reporting that you were surveilled at an overseas tradeshow	X			



Lightning Round! Question 7

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Failing to report that you were surveilled and solicited at an overseas tradeshow				



Lightning Round! Answer 7

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Failing to report that you were surveilled and solicited at an overseas tradeshow			X	



Lightning Round! Question 8

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Selling your programming job to a foreign actor that you don't know is a spy				



Lightning Round! Answer 8

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Selling your programming job to a foreign actor that you don't know is a spy			X	



Lightning Round! Question 9

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Staying late at work and working weekends, unexplained affluence, high use of copy machine, several security infractions				



Lightning Round! Question 9

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Staying late at work and working weekends, unexplained affluence, high use of copy machine, several security infractions			X	



Lightning Round! Question 10

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Whistleblower using proper procedures				



Lightning Round! Answer 10

Event	CI Only Concern	Insider threat, but not CI	Both!	Neither!
Whistleblower using proper procedures				X



CDSE CI Training and Job Aids

The FY19 CDSE Training Course Schedule is now available.

Plan your security training for the coming year. Sign up today!

CPI Short

Does your program have **Critical Program Information (CPI)**?
What are the consequences of compromise? Are you protecting CPI within your facility?

CDSE COUNTERINTELLIGENCE AWARENESS JOB AID

Foreign Collection Methods: Indicators and Countermeasures

IDENTIFY

- Identify the indicators
- Assess the indicators
- Identify the indicators

REPORT

- Reporting of Foreign Collection Methods is required under both the Intelligence Reform and Terrorism Prevention Act (IRTPA) and the Intelligence Reform and Terrorism Prevention Act (IRTPA).
- Failure to report can result in fines, prison, or both.

CDSE COUNTERINTELLIGENCE AWARENESS JOB AID

Counterintelligence Awareness Case Study: Attempted Acquisition of Technology – Radiation Hardened Integrated Circuits

Peter Zuccarelli – American Coasting Technologies

- 12 year old owner of Coast company
- August 3, 2011: First call to company to integrate and modify export controlled technology
- January 24, 2015: Surrendered to months in U.S. prison, three years supervised release, and \$50,000 fine for company to integrate and modify export radiation hardened integrated circuits (RHIC) to Russia and China, which is in violation of the International Economic Powers Act

What Happened?

- Between June 2011 and March 2015, Zuccarelli and co-conspirators agreed to illegally export RHICs to China and Russia.
- Zuccarelli and co-conspirators received purchase orders and payment of approximately \$1.5 million to acquire RHICs for Chinese and Russian customers, while claiming the company as the end user.
- Zuccarelli misappropriated RHICs and illegally shipped shipping documents to disguise the true identity of technology in order to illegally ship the export controlled technology without required licenses.

Impact

- Russia and China have significantly closed the gap in space platform technology with the U.S. through their aggressive and successful attempts in obtaining U.S. technology.
- Billions of dollars worth of U.S. technology was stolen annually through economic espionage.
- Radiation Hardened Integrated Circuits continue to be one of the most highly sought U.S. technologies.

CDSE COUNTERINTELLIGENCE AWARENESS JOB AID

Counterintelligence Awareness Case Study: Attempted Acquisition of Technology – Illegal Export to Iran

Alicia Jalaal

- 39 year old citizen of Iran
- March 20, 2015: Sentenced to 13 months in a U.S. prison for conspiracy to defraud United States by illegally exporting sensitive nuclear technology to Iran.

What Happened?

- Between 2009 and December 2013, Jalaal was a part time employee of Genes Wave Telecommunications, Inc. (Genes Wave), a Maldivian company located in Kuala Lumpur, Malaysia.
- Genes Wave Telecommunications operated as a front company for Fawaz Sidi Khatir (Fawaz SKK), an Iran based company that specialized in both hardware and software development.
- Genes Wave Telecommunications was used to illegally acquire sensitive export controlled technology from the United States on behalf of Fawaz SKK. In order to accomplish their acquisition, Jalaal and her co-conspirators provided the ultimate selling document and end users of the export technology through false statements, subverted financial transactions, and other means.
- The defendant's co-conspirators would contact producers and distributors of the sought after technology, who purchase agreements, and arrange for purchase and delivery of the goods under the alias. When the goods were received by Genes Wave Telecommunications in Maldives, Jalaal transported and subsequently exported for the Iran based Fawaz SKK in Tehran, Iran.

Impact

- In 2011, Fawaz SKK was designated by the United States Department of the Treasury as a Special Economic National for providing financial, technical, intelligence or other support, or goods or services in support of the Islamic Revolutionary Guard Corps (IRGC).
- The U.S. Treasury Department has sanctioned the designated end users of this technology due to their role in the illicit transfer of technology and in their use of technology to be used in weapons production systems.

CDSE COUNTERINTELLIGENCE AWARENESS JOB AID

Counterintelligence Awareness Case Study: Attempted Acquisition of Technology: Front Companies

Art Equibson – Alexander Fishenko

- Born U.S. Russian citizen
- Immigrated to U.S. in 1994 and became U.S. citizen in 2003.
- Founder (2005) and CEO of the American Int. Inc. (American Int.), an company to produce technology for satellite systems.

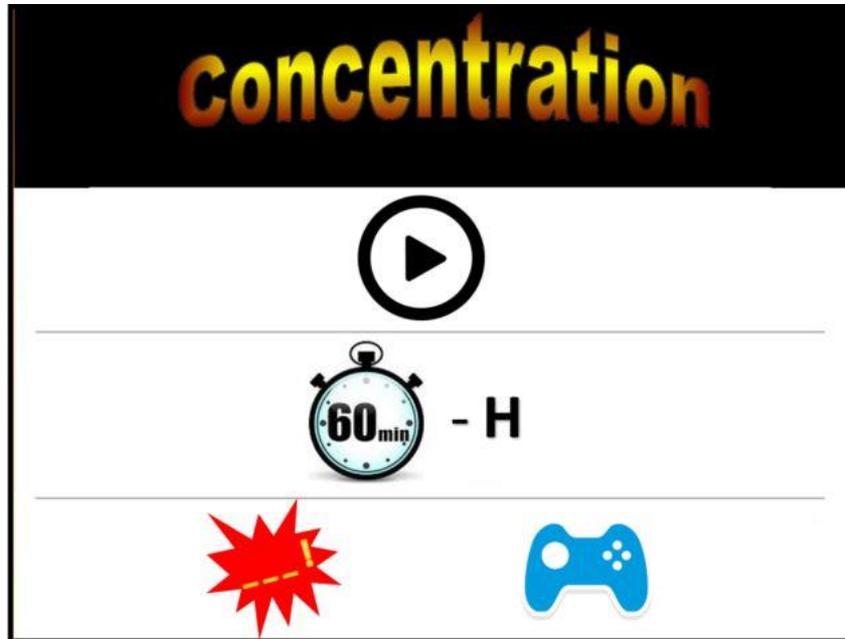
What Happened?

- Between October 2002 and October 2010, Art Equibson allowed to illegally export about \$20 million of advanced microelectronics from manufacturers and suppliers located throughout the United States to the Russian Ministry of Defense.
- Provided false and/or incomplete information in connection with the purchase of the goods, concealed the fact that they were restricted, and falsified the goods they exported to records submitted to the Department of Commerce.
- Equibson acted solely by acting as an agent of the Russian government, conspiring to and illegally exporting controlled microelectronics to Russia, acting as a front company, and distribution of such.
- Customers included the Russian Federal Security Service (FSS) or GRU.
- Customers included a research unit by the Russian FSB named security agency, a Russian entity that builds and installs defense systems and another that produce electronic warfare systems for the Russian Ministry of Defense.
- Completed in October 2010, he was sentenced to 180 months in prison and forfeited over \$200,000.

Impact

- Technology sent to Russia has military custom applications, including radar and communications systems, missile guidance systems, and navigation systems, none of which Russia does not produce domestically.

NEW VIGILANCE CAMPAIGN MATERIAL



VIEW MORE MATERIAL HERE:

<https://www.cdse.edu/toolkits/insider/vigilance.html>



CDSE

CDSE WANTS TO HEAR FROM YOU!

CDSE Counterintelligence POC:

Ed Kobeski

410-689-7842

EMAIL: Edwin.f.Kobeski.civ@mail.mil

