



CDSE

Center for Development
of Security Excellence

Security Speaker Series

Counterintelligence Support to Foreign Visits and Academic Solicitation

LEARN.
PERFORM.
PROTECT.

Today's Session:

Host: Mark Zahner, CDSE Counterintelligence

Guest Speaker: Special Agent Justin Shanken,
Defense Security Service



Foreign Visits and Academic Solicitation

AGENDA

What is it and why is it important?

What are they targeting?

What are the primary methods of exploitation?

Countermeasures we can employ

What and who to report information to

Foreign Visits: A foreign national enters or proposes to enter a DoD Component or cleared contractor facility or to meet with employees or representatives of the facility. There are two types of Foreign Visits, Official and Unofficial.



Academic Solicitation: Academic Solicitation as the use of students, professors, scientists or researchers as collectors improperly attempting to obtain sensitive or classified information.



What are they targeting?

- Research and Development information
- Personnel information
- Contracting information
- Security information
- Classified, sensitive,, or export-restricted basic and applies research
- Developing defense or dual-use technologies
- Information about the students, professors, and researchers working on the technologies

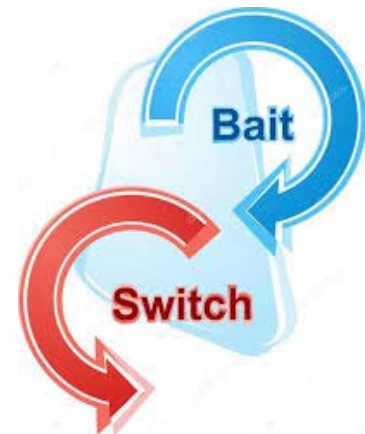
Who are they targeting?

- Subject Matter Experts
- Researchers and scientists
- Cleared contractors and businesses
- Academics



What are the primary methods of exploitation?

- Peppering
- Wandering Visitor
- Divide and Conquer
- Switch Visitors
- Bait and Switch
- Distraught Visitor
- Prohibited Electronics
- and many more...



Countermeasures

- Brief and train all escorts
- Develop standard practices and rehearse them
- Submit the names of the visitors to DSS prior to the visit
- Conduct pre-visit facility walk through
- Have a plan,,,



What to report

- Suspicious applications or requests for research positions
- Unsolicited request for assistance or information
- Unsolicited invitations to attend and/or present at international conferences
- Any line of questioning concerning military or intelligence based contracts or dual-use technology, unless previously approved.



Summary

What Foreign Visits and Academic Solicitation is
What they want
Methodology
Countermeasures
Reporting



Counterintelligence Training

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

Summary 1

Foreign collection methods, indicators and countermeasures are critical to the success of a counterintelligence program. This job aid provides a comprehensive overview of these concepts and offers practical guidance on how to identify and mitigate risks.

Summary 2

This counterintelligence job aid contains a list of 50 foreign collection methods, indicators and countermeasures. It is designed to help you identify and mitigate risks to your program.

Summary 3

This counterintelligence job aid contains a list of 50 foreign collection methods, indicators and countermeasures. It is designed to help you identify and mitigate risks to your program.

CDSE COUNTERINTELLIGENCE AWARENESS JOB AID

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

Peter Zaccarelli - American Coating Technologies

What Happened?

Between 2011 and 2013, Zaccarelli and his colleagues acquired highly sensitive information and technology from American Coating Technologies (ACT) in order to develop a competing product. This information was then used to develop a competing product that was sold to the same customers as ACT's product.

Impact

ACT's loss of sensitive information and technology resulted in a significant loss of competitive advantage. The company's market share was significantly reduced, and its financial performance was negatively impacted.

CDSE COUNTERINTELLIGENCE AWARENESS JOB AID

Counterintelligence Awareness Case Study: Attempted Acquisition of Technology - Legal Export to Iran

Alireza Jafari

What Happened?

Between 2010 and December 2011, Jafari was a joint law employee of Texas Instruments and a law firm in Houston, Texas. He was involved in the export of technology to Iran. This technology was used by Iran to develop its nuclear program.

Impact

The export of technology to Iran by Jafari and his colleagues resulted in a significant loss of competitive advantage for Texas Instruments. The company's market share was significantly reduced, and its financial performance was negatively impacted.

CDSE COUNTERINTELLIGENCE AWARENESS JOB AID

Counterintelligence Awareness Case Study: Attempted Acquisition of Technology - Smart Components

Ali Electronics - Alexander Vukobratovic

What Happened?

Between 2010 and 2013, Vukobratovic and his colleagues acquired highly sensitive information and technology from Ali Electronics in order to develop a competing product. This information was then used to develop a competing product that was sold to the same customers as Ali Electronics' product.

Impact

Ali Electronics' loss of sensitive information and technology resulted in a significant loss of competitive advantage. The company's market share was significantly reduced, and its financial performance was negatively impacted.

Counterintelligence Training

eLearning

- CI Awareness and Reporting Course
- Protecting Your Facility's Technology
- CI Foreign Travel Brief

Webinars/ Shorts

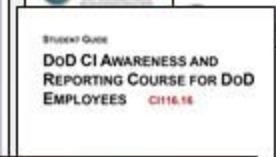
- Critical Program Information
- CI Awareness for Freight Forwarding
- Suspicious Emails

Job Aids

- CI Awareness Vigilance Campaign
- Industrial Base Technology (IBTL)

Toolkits

- Awareness and Training
- Reporting Requirements
- Supply Chain Risk Management



CDSE

Center for Development
of Security Excellence

Counterintelligence Training POC:

Mark Zahner

410-689-1135

Email: mark.e.zahner.ctr@mail.mil