Counterintelligence Awareness and Reporting for NAESOC Facilities

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Overview

- Mission & Vision
- Define Counterintelligence (CI)
- Protecting U.S. Technologies
- Threat Vectors
- Counterintelligence Awareness
- What To Do If Approached
- Potential Espionage Indicators
- Identifying Suspicious Contacts
- Reporting Procedures

Mission & Vision

Mission

DCSA is a strategic asset to our Nation and allies - continuously ensuring a trusted federal, industrial, and affiliated workforce, and enabling industry's delivery of uncompromised capabilities by leveraging advanced technologies and innovation. We uniquely blend critical technology protection, trusted personnel vetting, counterintelligence, and professional education and certification to advance and preserve America's strategic edge.

Vision

Guardians of our Nation's assets - ensuring trust, countering threats and vulnerabilities, and advancing delivery of uncompromised technology.

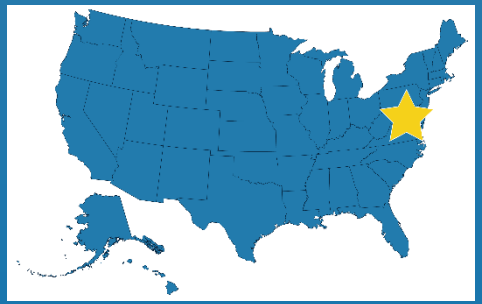
NAESOC

The **National Access Elsewhere Security Oversight Center (NAESOC)** is a centralized office providing consistent oversight and security management for select facilities who do not possess classified information on-site ("access elsewhere").

- **NAESOC Coordinates:** Communications, guidance, and education to facilities and government partners.
- **NAESOC Provides**: Continuous outreach and consistent direction.
- **NAESOC Results in:** Improved communications, threat reporting, vulnerability identification, and vulnerability mitigation

More information: https://www.dcsa.mil/mc/ctp/naesoc/

Contact the NAESOC Knowledge Center: (888) 282-7682, **option 7** (NAESOC)



The centralized NAESOC provides the most effective method for supporting security oversight for select access elsewhere facilities in the NISP.

- One voice for the director—one resource for the customer
- Leverages Continuous Evaluation vetting
- New training approach for non-possessors

What is Counterintelligence?

- Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against:
  - Espionage
  - Other intelligence activities
  - Sabotage
  - Assassinations

- Counterintelligence adversaries include:
  - Foreign powers
  - Foreign governmental and commercial organizations
  - Foreign persons or their agents
  - International terrorist organizations

What You Know

- You have access to classified information and/or information pertaining to technologies that are highly sought after by foreign entities

Friendly information

Research, development, testing, and evaluation

Program milestones & specifications

System capabilities

- Foreign entities will also target information relating to your facility's personnel, security, and operations

YOU are the first line of defense in protecting classified information and defense technologies!

External or Internal Threats

External (Cyber Actors, FIE)

- Cyber Operations
- Targeting U.S. Travelers Overseas
- Request for Information (RFI)
  - Attempted Acquisition of Technology
- Academic Solicitation
- Seeking Employment
- Exploitation of Relationships
- Solicitation or Marketing Services
- Joint Venture or Business Development

Internal

(Employee, Intern, Visitor)

Insider Threat

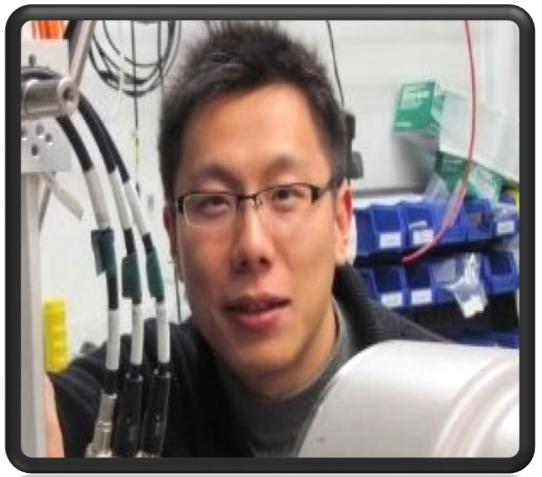
- Volunteers
- Sleeper Agents
- Co-opted Individuals

External or Internal Threats

Case Studies

Deepanshu Kher

Wei Sun



Hongjin Tan

CI Awareness - Insider Threat

Insider Threat – a person with authorized access who uses that access wittingly or unwittingly to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of recourses or capabilities. *(DoDI 5240.26)*

Indicators – observable actions, outside the norm, that can be seen or noticed through day to day activities by a co-worker.

Anomalies – foreign power activity or knowledge, inconsistent with the expected norm, that suggest foreign knowledge of U.S. national security information, processes, or capabilities. *(O-DoDI 5240.02)*

CI Awareness - Research & Academia

- Foreign entities often try to establish business or academic relationships with cleared facilities
  - Seeking employment
  - Solicitation or marketing services
  - Academic solicitation
    - Students attempting to work on research projects involving targeted technologies, and academics submitting research papers for review
  - Exploitation of relationship
    - Joint ventures and research provide opportunity to build rapport with and elicit information from cleared employees
- Practical countermeasures

CI Awareness - Research & Academia

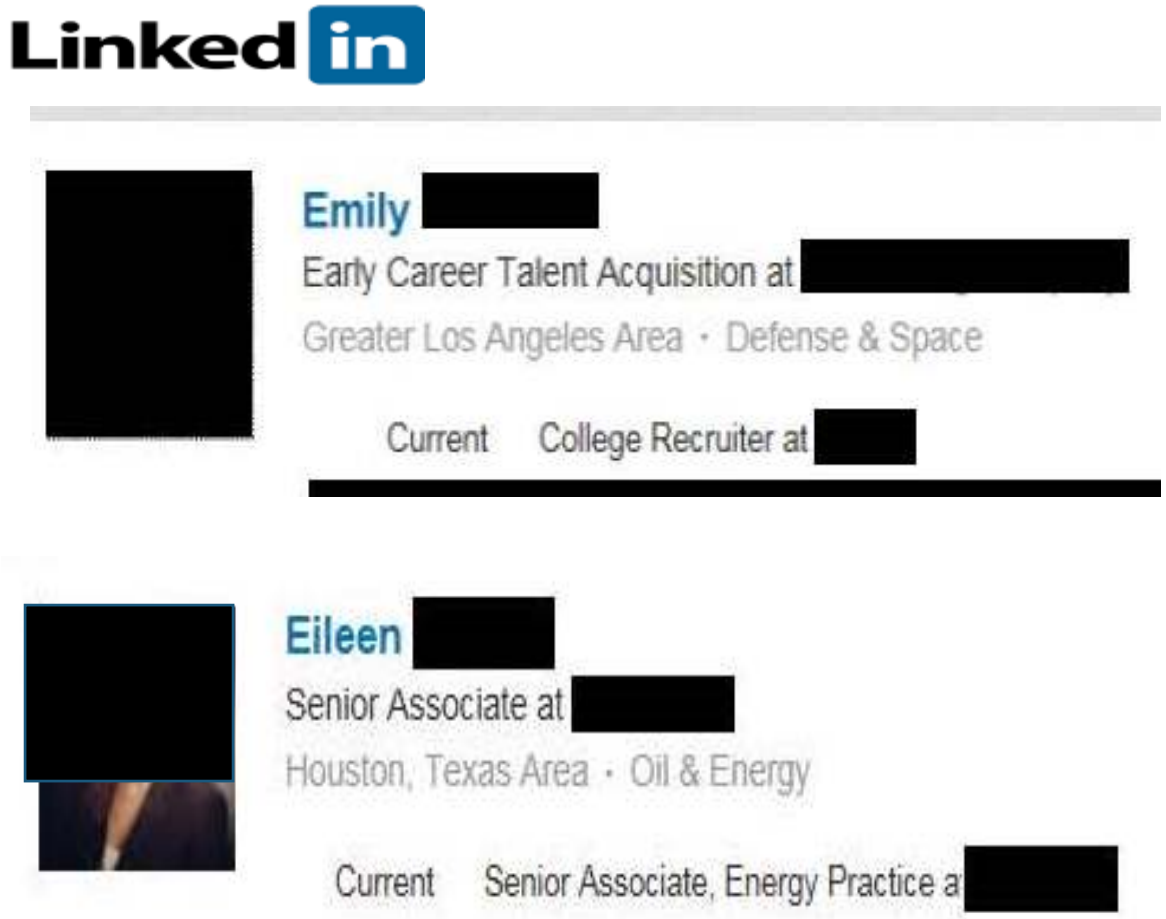
"The United States remains the top host of international students globally. International students made a significant financial impact on the United States in 2017, contributing $42.4 billion to the U.S. economy through tuition, room and board, and other expenses, according to the U.S. Department of Commerce."

https://www.iie.org/Why-IIE/Announcements/2018/11/2018-11-13-Number-of-International-Students-Reaches-New-High

CI Awareness - Social Media

- Social media is a growing area of vulnerability for individuals and cleared industry
- Social Networking Services (SNS) provide a new tool for foreign intelligence services to collect information on individuals, their work, and their families
- SNS are also vectors for hackers to load malicious content
  - Nearly half the “millennial” generation use SNS while at work
  - Hackers can use message applications or wall postings to create malicious links within the social networking sites
- Other criminals, including identity thieves, use SNS to gain information on likely targets

CI Awareness - Social Media



CI Awareness – Social Media

To: [Cleared Contractor Employee]
From: Emily [Spoofed Cleared Contractor Employee] <REDACTED@gmail.com>
Date: 12 Apr 2017 06:23:13 -0700

- Attempts to Impersonate as another Cleared Contractor

Dear [Cleared Contractor Employee],

I came across your profile on LinkedIn and thought you may be interested in learning more about our Electrical Engineer Manager position at [Impersonating as Cleared Contractor Facility]. I would like to discuss the details of this position we have available as well as review your future job goals. If you are no longer looking for a new position, or are not interested, please <*click here*> <http://link.gmgb4.net/x/o?u=3Da628cce7> to opt out.

- Contains Suspected Malicious URL
- Impersonating as another Cleared Contractor for Recruitment
- Incorrect Grammar

Your experience matches well and I would encourage you to take a look at the opportunity. Please reply today by e-mailing me and be sure to attach the most current copy of your resume.

We look forward to receiving your respond.

Thank you,

Emily [Spoofed Cleared Contractor Employee]
Talent Acquisition Recruiter
[Impersonating as Cleared Contractor Facility]

- FIE is utilizing an actual employee's name that works for another cleared contractor (in this position)

CI Awareness – Social Media

To: [Cleared Contractor Employee]
From: Eileen [SPOOFED UNCLEARED EMPLOYEE NAME]
Date: Thu, 27 Apr 2017 09:53:12 -0400

- Attempts to Impersonate as current employee of another cleared contractor

Hi Scott,

Thanks for the reply.
Please review the Job Description file
<https://deltaemis[.]com/CRCForm/3E_Company/<REDACTED>/L1754/Job%20Description.doc>

- Contains Malicious Hyperlink
- Beacons to Known FIE Infrastructure
- Downloads executables to victim's computer

As you can see, I think this role is an ideal match for your skills and experience.
If you are interested in this position, please let me know a convenient time for a phone conversation to go over details.

Kind regards,
Eileen [Spoofed Cleared Contractor Employee]
Senior Associate
[Impersonating as Employee Working for Actual Cleared Contractor]

- Impersonating as an Employee of Current Cleared Contractor
- Victim would believe this is legit if researching individual

CI Awareness – Cyber Security

- Foreign actors increasingly use computer network exploitation to obtain information relating to U.S. technologies
- Methods of exploitation
  - Emails with malicious links or attachments
  - Spoofing email addresses
  - Network software and website vulnerabilities
  - Removable media
- Practical countermeasures

CI Awareness - Foreign Visitors

- Foreign delegation visits to cleared contractors are a common method of operation used to target U.S. technologies
- Foreign visitor techniques
  - Peppering escorts/personnel with questions
  - Wandering
  - Practicing “divide and conquer”
  - Switching visitors
  - Making last-minute additions to visit request
  - Switching topics
  - Purporting to be “distraught”
- Practical countermeasures

CI Awareness - Foreign Travel

- Foreign travel increases the risk of foreign intelligence targeting
- Collection techniques
  - Bugged hotel rooms or airline cabins
  - Intercepts of fax and email transmissions
  - Tracking activity via ATM transactions and Internet usage at Internet kiosks or WIFI access points
  - Recording of telephone conversations
  - Unauthorized access to or theft of electronic devices – installation of malicious software
  - Intrusion into or searches of hotel rooms and hotel room safes
  - Enhanced interviews by customs officials
- Practical countermeasures

CI Awareness - Conferences, Conventions, and Trade Shows

- Conferences, conventions, and trade shows present collectors with a target-rich environment due to the abundance of technology, engineers, and technical personnel in attendance
- Collection techniques
  - Elicitation of classified or export-restricted information from subject matter experts
  - Theft of technology on display
  - Photography
  - Collection of business cards and other personal information
  - Gaining access to personal or business electronic devices left unattended
- Practical countermeasures

Potential Espionage Indicators

- Historically, espionage and terrorism subjects exhibit one or more of the following indicators:
  - Foreign contacts (unreported or attempts to conceal)
  - Foreign preferences/allegiance
  - Security violations
  - Financial concerns
  - Polygraph results (inconclusive or indicate deception)
  - Employment behaviors
  - Personal conduct
  - Foreign travel

Key: Identification of potential espionage indicators involves recognizing a pattern of suspicious activity

Identifying Suspicious Contacts

- Examples of suspicious contacts
  - Requests for protected information under the guise of a price quote or purchase request, market survey, or other pretense
  - Foreign entities targeting cleared employees traveling overseas via airport screening or hotel room incursions
  - Attempts to entice cleared employees into situations that could lead to blackmail or extortion
  - Attempts by foreign customers to gain access to hardware and information that exceeds the limitations of the export licenses on file
  - Attempts to place cleared personnel under obligation through special treatment, favors, gifts, or money

What To Do If Approached

- If you feel you are being solicited for information:
  - Practice authorized responses to questions concerning your duties
  - Never feel obligated to answer questions that make you feel uncomfortable
  - Change the topic of any conversation that might be too probing with respect to your duties, private life, and coworkers
  - Be observant:
    - Try to note as much as possible about the person asking questions
  - Maintain professional composure
  - **Report, Report, Report**:
    - Provide as much information as possible to your Facility Security Officer (FSO) about the encounter and the individual(s) involved

Reporting Cycle

Employee Identifies and Reports Suspicious Incident

FSO

Suspicious Contact Report (SCR)

1-302

Local CISA

NAESOC

Suspected Espionage

1-301

1-301

FSO

Evaluate Products
Adjust CI Program
Employee Feedback
Refine Briefings

Initial Evaluation/Screening and Feedback to FSO (Email)

FBI

Local /Federal Counterintelligence and Law Enforcement Agencies

Referrals

SCR

DCSA Intel Division (HQ)

Tailored Threat Products

NAESOC

Threat Based CI/Security Services

SCR analytical feedback

Additional Tools & Support

- Contact DCSA CI for questions regarding:
  - CIAR Briefing
  - Foreign Travel
  - Counterintelligence Support
  - Foreign Visitors
  - Arranging Briefings

- Center For Development of Security Excellence (CDSE) https://www.cdse.edu

Contact Information

National Access Elsewhere Oversight Center
Defense Counterintelligence and Security Agency

SA Mike Degnan
Michael.j.Degnan.civ@mail.mil
410-689-2990

NAESOC Help Desk
dcsa.naesoc.generalmailbox@mail.mil
1(888) 282-7682, option 7