

COUNTERINTELLIGENCE

Best Practices for Cleared Industry



WHAT IS THE THREAT?

U.S. cleared industry is a target of many foreign intelligence collectors and economic competitors. Industry threat reporting suggests a concerted effort to exploit cleared contractors (CCs) by overt attempts to steal technology, as well as covert business and academic ventures. DCSA's industry reporting analysis found foreign adversaries and competitors use traditional and nontraditional collectors and commercial and government-affiliated entities. The amount of commercial contacts reported likely represents foreign governments' attempts to make contacts innocuous by using non-threatening approaches.

WHO IS BEING TARGETED?

Anyone with access to targeted information, knowledge of information systems, or security procedures:

- **Developers:** Research and develop leading technologies
- **Technicians:** Operate, test, maintain, or repair targeted technologies
- **Supply Chain Personnel:** Source and purchase components integrated with deliverable defense products or technology
- **Information Systems Personnel:** Access to cleared facility networks and knowledge of network security protocols
- **Business Development Personnel:** Marketing/sales representatives for both domestic and foreign markets
- **Human Resources (HR) Personnel:** Access to sensitive information serving as public company contacts and initial screeners of prospective and current employees
- **Foreign Access Points:** Foreign travelers, foreign visitor hosts/escorts, and personnel with foreign contacts
- **Senior Managers:** Company owners and managers listed on open source web content and business records

- **Subject Matter Experts (SMEs):** Involved with targeted technology publishing in technical journals, participating in professional associations and/or academia, and patent owners
- **Administrative Staff:** Access to leadership calendars, contact lists, and company proprietary information
- **Janitorial, Maintenance, and Support Staff:** Access to personnel, information, and technology
- **Anyone with access to national defense information**

HOW ARE YOU BEING TARGETED?

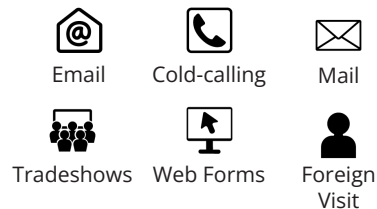
MOST COMMON METHODS OF OPERATION



ATTEMPTED ACQUISITION OF TECHNOLOGY:

Acquiring controlled technologies, via direct contact or through the use of front companies or intermediaries, including equipment, diagrams, schematics, plans, or product specification sheets.

METHODS OF CONTACT:



INDICATORS OF SUSPICIOUS PURCHASE REQUESTS:

- Similar name or address to those on government suspicious entities lists
- Suspicious delivery addresses: obscure addresses or multiple businesses using the same address
- Solicitor acting as procurement agent for foreign government
- Requesting commercial technology modified for military use
- Customer is reluctant to discuss item's end-use
- Customer line of business does not fit product's applications
- Customer wants to pay cash for an expensive item when sale terms would normally call for financing
- Customer has little to no business background available
- Customer declines routine installation, training, or maintenance/warranty services
- Customer is unfamiliar with product performance characteristics but still wants the product
- Customer uses third-party broker or address is listed in a third country



EXPLOITATION OF BUSINESS ACTIVITIES:

Establishing or leveraging a commercial relationship via joint ventures, partnerships, mergers and acquisitions, or foreign military sales to obtain controlled unclassified information (CUI).



EXPLOITATION OF SUPPLY CHAIN:

Compromising supply chain by introducing counterfeit or malicious products or materials into the supply chain to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communications.

Contact methods involve solicitations and marketing offers with below-average pricing and lead times; attempts to purchase a product line supplier; cyber operations; and exploitation of third-party technical service providers.



REQUESTS FOR INFORMATION (RFI):

Collecting protected information by eliciting personnel for protected information and technology.

METHODS OF CONTACT



Email



Telephone



Web Form



Foreign
contact, visit,
or travel



Conferences,
Conventions,
or Tradeshows



EXPLOITATION OF INSIDER ACCESS:

Trusted insiders exploiting authorized placement and access (P&A) within cleared industry or causing other harm to compromise personnel or protected information and technology.



EXPLOITATION OF CYBER OPERATIONS:

Foreign intelligence entities (FIEs)/adversaries compromising confidentiality, integrity, or availability of targeted networks, applications, credentials, or data to gain access to, manipulate, or exfiltrate personnel information or protected information and technology.

COMMON CYBER OPERATION METHODS:

- **Phishing Operations:** Emails with embedded malicious content or attachments for the purpose of compromising a network, including spear-phishing, cloning, and whaling
- **Exploitation of Mobile Devices:** Tampering with mobile devices that have trusted access to a protected network
- **Patch Management:** Attacks that exploit outdated networking equipment and unpatched software/hardware vulnerabilities
- **Watering Hole:** Use of a compromised website to target visitors, including third-party or company websites to access your customers or persons with common interests
- Introduction of Backdoor Access Panels

COUNTERINTELLIGENCE AWARENESS AND REPORTING



EXPLOITATION OF EXPERTS:

Gaining access to obtain CUI.

Contact methods include soliciting SME participation in foreign conferences or paying SMEs to collaborate with foreign academic institutions.

TRAINING REQUIREMENTS

CCs are required to receive training on threat awareness, counterintelligence (CI) awareness, and reporting requirements per National Industrial Security Program Operating Manual (NISPOM).



WHAT IS ELICITATION?

Elicitation is a structured Method of Contact (MC) communication to extract predetermined information; the subject is unaware they are a target. The elicitor will attempt to conduct collection activities away from the target's work to be less security conscious to ease the elicitation process. Because elicitation can sound like a common conversation, it is difficult to tell if it is a friendly conversation or intelligence gathering. FIEs look for professional and personal information to use in future targeting efforts. Elicitation requires patience and persistence. Pieces of information, collected over an extended period, gives the adversary desired information about technology, programs, and processes.

HOW ARE YOU BEING TARGETED?

- **Exploitation of Tendency to Complain:** Statements such as "I am so behind at work" can elicit a cleared employee's response, divulging schedule setbacks, staffing shortfalls, resource shortages, and other valuable information to a foreign government or competitor
- **Questionnaires and Surveys:** An elicitor states a benign purpose for the survey and surrounds questions they want answered with logical questions
- **Feigning Ignorance:** An elicitor portrays ignorance to have the target instruct them about a topic. This tactic is frequently employed in academia; it exploits the habit of teaching and puts the target in a familiar mindset to share information
- **False Statement:** An elicitor knowingly makes a false statement so the target can correct them. Another example is citing someone else's research or paper; this is particularly effective if the target is knowledgeable about the study/research area
- **Flattery:** Statements such as "That thing is really cool" can elicit numerous responses by leading the target to converse about topics of interest
- **Quid Pro Quo or Trading Confidences:** The elicitor provides the target with valuable information. Conversations begin, "I shouldn't tell you this but" or "This is off the record." This induces the target to return the favor and provide valuable information. Espionage may look more like a business transaction and less like gathering information
- **Paper Review:** Many cleared employees have ties to academia and research institutions. Cleared employees regularly receive requests to peer review research or theses. Many requests are straightforward, but some are attempts to leverage sensitive or classified research
- **Bracketing:** An elicitor asks a target about a sensitive value using high and low values, rather than asking for a specific number. The elicitor asking if the range is somewhere between 10 and 15 kilometers garners a response such as "Yes, in the high end." Bracketing allows the elicitor to adjust the bracket for the next target
- **Oblique Reference or Analogies:** An elicitor discusses a topic similar to the target's work so the target will use their work to make a point of reference. An example is the elicitor discussing a foreign or civilian system similar to the target's work. The target is likely knowledgeable and comfortable discussing this topic. The target may slip and use their own sensitive system as a point of reference to the foreign system
- **Criticism:** Criticism is accomplished by criticizing the target. An example is statements such as, "I saw on the news" or "I heard," followed by a statement that criticizes the cleared employee's work, company, or project. Many people will defend things they feel passionate about

WHY IS ELICITATION EFFECTIVE?

Elicitors will try to exploit natural human tendencies:

- Desire to seem polite and helpful
- Desire to seem knowledgeable or well-informed
- Desire to seem competent
- Desire to feel appreciated and contribute to something important
- Gossiping
- Correcting others
- Underestimating information's value
- Believing others are honest
- Complaining
- Showing empathy
- Being indiscrete, especially when emotionally charged

COUNTERMEASURES

In the event you are targeted, be prepared to respond. Know what information you cannot share and be suspicious of those seeking information. Do not share anything the elicitor is not authorized to know, including personal information. If you believe someone is attempting to elicit information from you:

- Change the topic
- Refer them to public websites
- Deflect the question with one of your own
- Provide a vague answer
- Explain that you don't know, and respond with "Why do you ask?"

Consider: If you have to say "No" let your FSO know.

WHAT TO REPORT

Elicitation is a suspicious contact reportable by cleared companies to DCSA under the NISPOM.

EXAMPLES OF REPORTABLE ACTIVITY

- Any individual's efforts, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee
- All contacts with known or suspected intelligence officers from any country
- Any contact that suggests an employee may be targeted for exploitation attempts by another country's intelligence services

Because elicitation is subtle and difficult to recognize, report suspicious conversations to your FSO, DCSA Industrial Security Representative, and DCSA CI Special Agent. These individuals can assess the information and determine if a potential CI concern exists.



WHAT IS PERSONAL CONTACT?

Personal contact occurs when a foreign actor, agent, or recruiter is in direct or indirect contact with a target.

FIEs commonly use elicitation to collect intelligence through contact that appears routine. A FIE Method of Operation (MO) attempts to confirm or expand knowledge of a sensitive program or gain clearer insight into a person's P&A prior to possible recruitment.

WHO IS BEING TARGETED?

Anyone with access to classified or sensitive intelligence. FIEs target anyone with P&A to desired information, knowledge of information systems, or awareness of security procedures.

This includes:

- **Developers:** Research and apply new materials or methods to Department of Defense (DoD) programs and technologies
- **Technicians:** Operate, test, maintain, or repair targeted technologies
- **Production Personnel:** P&A to targeted technologies' production lines or supply chains
- **Information Technology (IT) Personnel:** Access to targeted facility networks and knowledge of network security protocols
- **Business Development Personnel:** Marketing and sales representatives, business travelers
- **Human Resources Personnel:** Access to personnel records and job applicants
- **Facility Employees:** P&A to a cleared or sensitive facility containing targeted information, including security, clerical, maintenance, and janitorial personnel

HOW ARE YOU BEING TARGETED?

PRIMARY METHODS OF OPERATION



Exploitation of Business Activities



Exploitation of Insider Access



Search/Seizure



Exploitation of Security Protocols



RFI/Solicitation



Exploitation of Relationships

HOW CAN YOU RECOGNIZE IT?

This approach is usually subtle. Some indicators include:

- Business contact requesting information outside contract scope or through an increased or gradual progression of information initiated from legitimate discussions
- Request to move communications to platforms outside official business channels, such as commercial chat
- Hidden/obscured end use/end user data
- Offer of paid attendance at an overseas conference; keynote or guest speaker invitations
- Casual acquaintance appears to know more about your work or project than expected
- Casual contact shows unusual interest in your work, facility, personnel, or family details

WHY IS PERSONAL CONTACT EFFECTIVE?

Foreign intelligence officers (IOs) are trained in elicitation tactics and operate without borders. Non-traditional collectors, such as business and academic contacts, leverage existing relationships to obtain restricted information outside the relationship scope. Not all elicitation attempts are obvious. IOs and non-traditional collectors assess and leverage the target's personal goals and vulnerabilities to elicit information.

Elicitation should be reported even if there is no intent to reconnect.

Trained IO elicitors and non-traditional collectors will try to exploit natural human tendencies, including:

- Being polite and helpful
- Appearing well-informed, especially about your profession
- Expanding discussion on a topic, likely giving praise or encouragement
- Correcting others
- Underestimating the value of information being sought or given
- Believing others are honest

COUNTERMEASURES

In the event a personal contact requests restricted information or attempts to place you in an exploitable situation, be prepared to respond. Know what information you cannot share and be suspicious of those who seek such information. Do not share anything the elicitor is not authorized to know, including personal information about yourself or coworkers. Outreach may occur via social media. Plan tactful ways to deflect probing or intrusive questions. Never feel compelled to answer any question that makes you uncomfortable.

If someone is attempting to elicit information:

- Change the topic
- Refer them to public websites
- Deflect the question
- Provide a vague answer
- Have a prepared canned answer
- State that you do not know

Consider: If you have to say "No" let your FSO know.

PERSONAL CONTACT

WHAT TO REPORT

Personal contact is the vector for many intelligence MOs that constitute suspicious contact. Report any suspected instance of actual or attempted elicitation.

EXAMPLES OF REPORTABLE SUSPICIOUS CONTACTS

- Any individual's efforts, regardless of nationality, to obtain illegal or unauthorized access to sensitive or classified information or to compromise a cleared employee
- All contacts with known or suspected foreign IOs
- Any contact that suggests foreign intelligence services may be targeting an employee for exploitation
- Business contact requesting information outside contract/agreement scope
- Business/personal contact seeking information about your coworkers or job duties
- Business/personal contact requesting you to violate company policy or security procedures

Because elicitation can be subtle or requests from personal contacts seem harmless, report any suspicious conversations to your FSO or DCSA CI representative.

WHAT IS ACADEMIC SOLICITATION?

FIE collectors may attempt to use students, professors, scientists, or researchers to obtain sensitive or classified information.

Collectors may collaborate with U.S. research institutions under the guise of legitimate research to access developing technologies and cutting-edge research.

These attempts include requests for peer or scientific board reviews of academic papers or presentations; requests to study or consult with faculty members; and requests for software and dual-use technology.

Academic solicitation can also occur when a faculty member, student, employee, or visiting scholar seeks access to this same information.

The number of foreign academics requesting to work with classified programs is rising, and the academic community will likely remain a top target for the foreseeable future.

Although most academic contacts are legitimate, some foreign academics may take advantage of P&A to further their country's research and development goals.

WHO IS BEING TAGRETED?



Researchers, scientists, and SMEs:

- Conducting classified or controlled unclassified research/projects for U.S. Government customers
- Employed at cleared components of academic institutions or with CUI work published in scientific or technical journals or presented at conferences
- Working on cutting-edge technology



Students, professors, and researchers:

- Access to research and technical information (especially graduate and post-doctorate students)



SMEs: Teaching technical courses

WHAT IS BEING TARGETED?

- Classified, CUI, or export-restricted basic and applied research
- Information about military, defense, and intelligence research applications
- Developing defense or dual-use technologies
- Significant or important research-related information, including: prepublication research results; research data; laboratory equipment and software; access protocols; equipment specifications; proprietary research, formulas, and processes; prototypes and blueprints; and technical components and plans
- Information about students, professors, and researchers working on the technologies

WHY DO COLLECTORS USE THIS METHOD?

- Effective way to collect information due to collaborative nature of academics
- Exploit student access to supplement intelligence collection efforts against emerging Department of Defense (DoD) and civilian research
- Sending students to study at U.S. facilities provides educated scientists and researchers for country-specific technology development

**Researcher
Pleads Guilty to
Conspiring to Steal
Scientific Trade Secrets
from a Hospital to Sell in
China**

U.S. Department of
Justice, Office of
Public Affairs

VIGNETTES

- Foreign students accepted to a U.S. university or to a postgraduate research program receive state-sponsored scholarships from their home country's government/government-affiliated entity
- U.S. researchers receive requests to provide dual-use components under the guise of academic research
- U.S. researchers receive unsolicited emails from peers in their academic field soliciting assistance on fundamental and developing research
- U.S. professors or researchers receive unsolicited invitations to attend or submit a paper for an international conference
- Overqualified candidates seek to work as interns in cleared laboratories
- Candidates seek to work in cleared laboratories whose work is incompatible with the requesting individual's field of research
- Foreign scientists, academics, or researchers request a U.S. SME review research papers, in hopes the SME will provide information that assists with future research
- Request a foreign exchange program or one-for-one swap

Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China
U.S. Department of Justice,
Office of Public Affairs

COUNTERMEASURES

- Be familiar with FIE MOs
- Know and understand legal and institutional restrictions to research at your facility
- Ensure proprietary and controlled information is carefully protected
- Employ screening/vetting procedures before collaborating with unknown entities and conduct background checks on potential partners from foreign state-sponsored entities
- Adhere to information system security procedures and monitor computer networks routinely for suspicious activities or compromise
- When in doubt, report any questionable solicitation, engagement, or unusual activity to your institution's security official/FSO. Do not try to downplay or self-adjudicate the suspected interaction as it may be a small piece of information that completes the bigger picture

ACADEMIC SOLICITATION

WHAT TO REPORT

Any contact (i.e., emails, telephone, personal contact) that is suspicious because of the manner or subject matter of the request. This includes requests from U.S. persons or from foreign nationals located in the United States or abroad, and may consist of:

- Unsolicited applications or requests for undergraduate, graduate, postgraduate, or other research positions
- Unsolicited requests for access to research papers or other research-related publications or documents
- Unsolicited requests for assistance with or review of thesis papers, draft publications, or other research-related documents
- Unsolicited invitations to attend and/or present at international conferences
- Unsolicited grants or gifting of funds/equipment to conduct joint research projects from foreign academic institutions or foreign governments

WHAT IS THE RISK TO ACADEMIA?

Proper vetting of foreign students, foreign faculty, and visiting foreign researchers/scholars is essential to protecting vital research and development within U.S. academic institutions. Enhanced vetting efforts play a vital role in thwarting adversarial acquisition of research conducted at U.S. academic institutions. This job aid will educate and assist cleared academia on threats from foreign entities.

POTENTIAL IMPACTS:

- National security implications
- Enhanced threats against the warfighter (our loss is their gain)
- Loss of federal and state research funding
- Loss of intellectual property revenue
- Loss of endowments, gifts, donations, prestige, or loss of credit
- Loss of grants and contracts
- Regulatory fines, penalties, and criminal liabilities

WHO IS BEING TARGETED?

U.S. academic institutions, specifically U.S. Government Affiliated Research Centers and Federally Funded Research and Development Centers (FFRDCs), persist as a target of non-traditional collection of research and technology.

WHAT IS BEING TARGETED?

Information collection via academia allows adversaries to identify dual-use technologies and transfer proprietary research. Foreign adversaries continue to exploit the openness of U.S. academia and ongoing research as a means to transfer classified and unclassified information, CUI, and sensitive, export-controlled research to advance national security interests.

WHO SHOULD BE VETTED?

Non-immigrant students and visiting scholars associated with:

- Foreign military research or institutions
- Foreign government sponsorship
- Foreign government or military employment
- Scholarship requirements mandating internships with defense companies or contact with foreign diplomatic institutions
- Academic exchange agreements involving emerging or dual-use technology
- International cooperative programs for innovative talents and foreign influence

- Cultural Institutes

COUNTERMEASURES

• Use security/red-flag and export control lists to screen for restricted or denied parties, such as the Consolidated Screening List, located at www.trade.gov/consolidatedscreening-list. Any dealings with a party on these lists violates U.S. export/sanctions regulations and requires further authorization and approval from the respective government agency:

- » **Denied Person List:** Individuals and entities denied export privileges
- » **Unverified List:** End users Department of Commerce (DoC) is unable to verify
- » **Entity List:** Parties whose presence in a transaction can trigger a license requirement supplemental to those elsewhere in the Export Administration Regulations
- » **Military End User (MEU) List:** No license exceptions are available for exports, re-exports, or transfers (in-country) to listed entities on the MEU List
- » **Nonproliferation Sanctions:** Parties sanctioned under various statutes
- » **Arms Export Control Act (AECA) Debarred List:** Entities and individuals prohibited from participating in defense articles export
- » **Specially Designated Nationals List:** Parties who may be prohibited from export transactions based on the Treasury's Office of Foreign Assets Control (OFAC)

regulations

- If an individual or entity appears on these lists, contact your assigned DCSA CI Special Agent immediately
- Leverage vetting support from supporting Federal agencies. *Note: for non-U.S. persons only*
- Participate in the National Defense - Information Sharing and Analysis Center (ND-ISAC) to support identification and sharing of risk indicators
- Use publicly available information about foreign entities of concern to understand the potential risk of affiliations
- Scrutinize Curriculum Vitae (CV), resumes, and applications for red flag issues:
 - » False information
 - » Links to denied party screening indicators
 - » Similar or identical information to other applicants
 - » Affiliations with foreign military research or institutions from high-threat countries
 - » Research interest mismatches between applicant's declared interest and what reflects in the CV
- Review applicant's research publications for red flag issues using web resources
 - » Research topic conflicts between expressed interest and published work
 - » Military-related research topics and applications
 - » Coauthors affiliated with high-threat countries and/

FOREIGN VETTING IN CLEARED ACADEMIA

or links to denied party indicators and institutions

- Verify applicant's references listed in the CV or application
- Verify applicants declared contracts, grants, awards, etc., via www.researchgate.net/
- Use the Student and Exchange Visitor Information System (SEVIS), www.ice.gov/sevis, managed by DHS Immigrations and Customs Enforcement (ICE), to report student and visitor information, including suspicious activity. This allows derogatory information on a student and/or visitor to be tracked and monitored throughout the United States
- Leverage relationships with local and regional officials from the DCSA CI, Federal Bureau of Investigation (FBI), ICE and other federal law enforcement and security organizations for enhanced review and analysis of foreign applicants

WHAT ARE INSIDER THREATS?

Insider: Any person with authorized P&A to U.S. Government or contract resources to include personnel, facilities, information, equipment, networks, or systems. This can include employees, former employees, consultants, and anyone with P&A.

- » *Department of Defense Directive (DODD) 5205.16: Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD.*
- » *Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM): Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems.*

Insider Threat: The danger an insider will use P&A to harm U.S. security.

- » *DODD 5205.16: The threat an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.*
- » *NISPOM 32 CFR Part 117: 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.*

An insider can have a damaging impact on national security and industry, such as:

- Loss or compromise of classified information or CUI
- Weapons systems cloned, destroyed, or re-engineered
- Loss of U.S. technological superiority
- Economic loss or company bankruptcy
- Loss of company proprietary information
- Company's loss of a competitive advantage

WHY IS EXPLOITATION OF INSIDER ACCESS EFFECTIVE?

Information collection that previously took years now takes only minutes due to removable media.

Insiders are aware of company vulnerabilities and exploit that knowledge to their benefit. Not every suspicious circumstance or behavior represents an insider threat, but every situation should be examined to determine risks and exploitable vulnerabilities.

HOW CAN YOU RECOGNIZE AN INSIDER THREAT?

Identifying potentially malicious behavior involves gathering information from numerous sources and analyzing the data for concerning behaviors or clues. In most cases, co-workers admit they noticed suspicious or questionable activities, but failed to report incidents. They did not acknowledge insider threat patterns or did not want to get involved or cause problems. Their failures to dutifully report caused grave issues for their company. Reporting insider threats is a requirement, not a choice.

A single CI indicator may say little; however, when combined with other CI indicators, it can reveal a detectable behavior pattern.

Ignoring questionable behaviors only increases potential damage to national security and employee safety. While every insider threat's motives differ, CI indicators are consistent.

POTENTIAL RISK INDICATORS

- Repeated security violations or general disregard for security rules
- Failure to report overseas travel or contact with foreign nationals
- Seeking to gain higher security clearance or expand access outside job scope without need
- Engaging in classified conversations without need to know
- Allowing physical access to unauthorized individual(s) outside normal visitor procedures/business hours
- Attempting to enter classified or restricted areas without authorization
- Working hours inconsistent with job assignment or unusual insistence on working in private
- Accessing unnecessary information
- Asking sensitive questions outside need to know
- Accessing sensitive information on personally owned devices

BEHAVIORAL INDICATORS

These behaviors may also indicate potential workplace violence.

- Depression
- Excessive stress in personal life (perceived life crisis)
- Fiscal irresponsibility or financial distress
- Unexplained affluence

EXPLOITABLE BEHAVIOR TRAITS

- Abusive use of alcohol or illegal/prescription drugs
- Uncontrollable gambling
- Prior disciplinary issues

COUNTERMEASURES

We all face individual hardships; however, it is important to seek positive outcomes whenever possible. Ensure you and your colleagues get help when appropriate. You are the first line of defense against insider threats. Help protect our national security by reporting any concerning behavior that may be related to an insider threat.

Each employee is responsible for ensuring the protection of classified information and CUI entrusted to them.

Be aware of potential issues and actions of those around you and report concerning or anomalous behavior and activities to your local security official/FSO, as well as the insider threat program senior official.

WHAT TO REPORT

INFORMATION COLLECTION

- Keeping classified materials in an unauthorized location
- Attempting to access classified information without authorization
- Unauthorized use of removable media
- Obtaining access to sensitive information inconsistent with present duty requirements
- Questionable downloads
- Maintaining unauthorized backups

INFORMATION TRANSMITTAL

- Unnecessarily copying classified material
- Discussing classified materials on a non-secure telephone or in non-secure emails or texts
- Using an unclassified medium to transmit classified material
- Removing classification markings from documents

FOREIGN INFLUENCE

- Expressing loyalty to another country
- Concealing reportable foreign travel or contact
- Significant ties to family members in foreign countries

CCs are required to receive training on Insider Threat Awareness as per the NISPOM.

EXPLOITATION OF INSIDER ACCESS

WHAT ARE CYBERTHREATS?

Our nation's cyber adversaries have tools and tricks from a multitude of resources, including publicly available information on the Internet. This makes it difficult to differentiate between criminal and intelligence entities, exacerbated by the ease with which adversaries can obtain information about potential targets. We live in a world where the Internet of Things includes computers, cell phones, Smart TVs, Alexa, Ring, watches, satellite radio, refrigerators, and window shades.

WHO IS BEING TARGETED?



You

Any individual, cleared or uncleared, regardless of job title or position, who can be used to gain access to an unsuspecting organization's network



Your company

Any organization or company, cleared or uncleared, with access to information coveted by our nation's adversaries

WHAT IS BEING TARGETED?

- International Traffic in Arms (ITAR), export-controlled and critical technology, and CUI
- Research and development
- Company unclassified networks (internal and external), partner and community portals, commonly accessed websites, and unclassified search history
- Proprietary information
- Administrative and user credentials
- Patch update sequences/patterns

FIEs seek aggregates of CUI or proprietary documents which paint a classified picture.

HOW ARE YOU BEING TARGETED?

- **Information Gathering:** Harvesting information
- **Targeting:** Coupling exploit with delivery methods
- **Delivery:** Infecting the target commonly using email, website hijacking, and removable media
- **Exploitation:** Exploiting a vulnerability on a system to execute code
- **Installation:** Malware providing persistence on targeted network
- **Command and Control:** Remote access computers, networks, or software/firmware
- **Actions on the Objective:** Access targeted information, data, and technology

HOW ARE YOU VULNERABLE?

- Publicly available information
- Contract information
- Company websites with technical/program data
- Connections (partnerships, key suppliers, joint ventures, etc.) with other cleared or uncleared companies
- Employee association with companies or technologies made public through scientific journals, academia, social networking sites such as Facebook and LinkedIn, etc.

PERSISTENT AND EMERGING CYBER THREATS

- Deepfakes: Creating fake images, sounds, and videos to fool the viewer
- Poisoning Attacks: Malicious injection into artificial intelligence program while it is learning
- Ransomware: New tactics, techniques, and procedures to exfiltrate data and release to the public
- Supply chain vulnerabilities
- Unsecure security products
- Malicious code injection
- Botnets
- Brute force
- Social network sites
- Credential harvesting

COUNTERMEASURES

- Training
- Using complex passwords
- Educating employees on social networking and email targeting; phishing email signs and reporting
- Defense in depth
- Technical defenses
- Patch management
- Monitoring suspicious network activity
- Open lines of communication among facility security, CI, and network defense personnel
- Having a failsafe relating to system administrators. One person should not have all of the “Keys to the Kingdom”
- Proper configuration–audit and automate secure configuration

WHAT TO REPORT

- All cyberthreats
- Aggressive port scanning outside normal network noise
- Advanced techniques / evasion techniques
- Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading
- Social engineering, electronic elicitation, email spoofing, spear-phishing, whale phishing, or direct questioning
- Unauthorized network access
- Actual or attempted unauthorized access into U.S. information systems
- Tampering with or introducing unauthorized elements into information systems
- Unexplained storage of encrypted data
- Unexplained user accounts, administrator accounts, and expansion of network privileges
- Data exfiltration
- Malicious codes or blended threats
- Unauthorized email traffic to foreign destinations
- Use of DoD account credentials by unauthorized parties
- Network spillage incidents or information compromise
- Unauthorized transmissions of classified information or CUI
- Any cyberactivity linked to suspicious indicators provided by DCSA, or by any other cyber centers and government agencies

WHAT ARE FOREIGN INTELLIGENCE THREATS VIA SOCIAL MEDIA?

Social media provides FIEs vast opportunities to exploit personnel. FIEs attempt to obtain U.S. critical technology, proprietary data, advanced research and development (R&D), and other valuable U.S industry information.

WHO IS BEING TARGETED?



62.6%

5.07 billion people use social media, about 62.6% of the global population. Anyone on social media can become a target.*



2.5 hours

The average social media user spends 2.5 hours on social media every day, amounting to 12 billion hours daily across the globe.*



6.7 platforms

The average social media user visits 6.7 social media platforms each month.*

HOW ARE YOU BEING TARGETED?

FIEs actively exploit social media. Once posted, information is not private and cannot be deleted. Using robust privacy settings provides a layer of protection, but the information still resides on a server.

Social media sites collect information on account owners, which is used to tailor their experience. Depending on the site, information can be sold and analyzed.

FIEs and foreign competitors use social media to conduct collection activities:

- Request friends/professional connections
- Monitor social media accounts
- Elicit information
- Recruit assets

Techniques used to collect on social media are:

- Flattery
- Providing information to get information
- Finding commonality
- Targeting on professional social networking sites
- Obfuscation of true identity
- Résumés containing malware
- Detailed information makes an easy target for adversarial collectors
- Transition from social media to real world using guises: recruiting, speaking engagements, etc

ELICITATION

Elicitation is an effective technique adversaries use to subtly collect information. Elicitation is non-threatening and allows elicitors to easily distort facts and exploit human nature (to be polite, well-informed, appreciated, trusting, etc.).

DISINFORMATION

Adversaries spread misleading or false information via social media using fake bot accounts and troll farms. A troll farm is an organization whose employees or members attempt to create conflict and disruption in an online community. Social media uses algorithms that inadvertently amplify malicious content to users, causing a widespread false narrative. This gives adversarial countries potential influence of current events in the United States.

FAKE PERSONAS ON SOCIAL MEDIA

- Realistic online identities
- Purported commonalities such as company, school, research
- Potential connections to colleagues or friends via successful targeting
- Societal norm of an attractive individual
- Linked to the same company but in a different country

"Instead of dispatching spies to the U.S. to recruit a single target, it's more efficient to sit behind a computer in China and send out friend requests to thousands of targets using fake profiles."

William Evanina, Director,
NCSC

*According to Datareportal.com

COUNTERMEASURES

- Think before you post
- Limit or exclude personally identifiable information (PII)
- Disable geotagging
- Consider a pseudonym
- Create strong passwords; change often
- Never put sensitive or proprietary information or CUI on your social media profile
- Be wary of unsolicited messages
- Do not accept connections from unknown sources
- Do not click/download suspicious links or files
- Follow company security and information assurance policies

- Use caution accessing games, quizzes, and applications that access and mine user data
- Assume all posted material can never fully be deleted
- Read the social media site's policy to ensure full understanding of personal data collection
- Report suspicious contacts immediately to the FSO and DCSA
- Keep firmware up-to-date

FOREIGN INTELLIGENCE THREATS VIA SOCIAL MEDIA

**Loose lips sink ships.
Everyone is a target
when associated with
CC facilities, companies,
technology, R&D, etc.**

WHAT TO REPORT

- Questionable or suspicious contacts on social media platforms
- Any Social Networking Service (SNS) persona attempting to elicit information
- Suspected or known fake personas attempting to obtain specific information pertaining to your profession
- Suspicious files sent via private message
- Any attempt at click-jacking (concealing hyperlinks beneath legitimate clickable content) or malware
- RFIs, academic solicitation, or job offers from adversarial countries
- Unsolicited contacts from unknown individuals

WHAT IS EXPLOITATION OF BUSINESS ACTIVITY?

Establishing or leveraging a commercial relationship via joint ventures, partnerships, direct commercial sales, or service providers to obtain access to personnel, protected information, and technology.

WHO IS BEING TARGETED?

- Any cleared employee or cleared company that supports cleared facilities, works with CUI, or classified information related to the DoD or other U.S. Government programs
- Employees involved in business development, sales, marketing, information sharing, or professional collaborative efforts to develop a relationship
- Entities seek to leverage business relationships to contact other cleared employees working with targeted information and technology



HOW ARE YOU BEING TARGETED?

METHODS OF OPERATION:



- Cultural commonality
- Acquisition of technology via a cleared company's foreign sales representative or distributor



- Business propositions and solicitations
- Direct military or commercial sales



- Joint ventures
- Claiming to have been referred

METHODS OF CONTACT:



Email



Foreign Visits



Cyber Operations



Web Form



Personal Contact



Conferences,
Conventions, or
Tradeshows



Résumé—
Academic



Social Networking
Service

WHY IS EXPLOITATION OF BUSINESS ACTIVITY EFFECTIVE?

Foreign entities exploit legitimate activities with defense-oriented companies to obtain access to otherwise denied information, programs, technology, or personnel. This MO relies on the legitimacy provided by the established commercial or business activity. Conversely, U.S. personnel seeking to gain future business with foreign partners may unwittingly provide information beyond the scope of the original business activity.

EXAMPLES OF THIS EXPLOITATION MAY INCLUDE:

- Foreign ownership of, or financial interest in, a U.S. company may provide access to intellectual property rights held by the U.S. company
- Business activity may allow the foreign company access to information on U.S. networks
- Foreign-produced hardware and software may include design vulnerabilities and malware that could provide foreign actors access to a company's network
- Foreign collectors prey upon cleared employees' eagerness to develop commercial relationships to increase sales or revenues
- A joint venture with a foreign company using the U.S. company's name allows foreign employees to use the U.S. company's name on business cards
- Cleared employees unaware of commercial agreement security limits or export control restrictions may commit a security violation by unwittingly providing information that should not be shared

HOW CAN YOU RECOGNIZE IT?

A business relationship with a foreign company or person may be entirely legitimate; however, foreign entities with nefarious intent may abuse relationships with U.S. industry to establish pathways to restricted information and technology. Building on legitimate business activity, foreign collectors abuse the relationship as a vector to gain access to restricted or prohibited information. These commercial and business relationships include:

- Misrepresenting themselves as a foreign representative for a U.S. company
- Selling and installing hardware or software in CC or sensitive facility networks
- Buying a substantial or majority interest in U.S. companies to gain intellectual property rights for technology, sharing data, or appointing key management personnel in the acquired company

VIGNETTES

- Foreign company has a nebulous business background
- Foreign company attempts to obscure ties to foreign government
- Foreign company attempts to acquire interest in companies or facilities inconsistent with current business lines
- Foreign partner/client requests to visit cleared facility not related to the business relationship
- Foreign visitors violate security protocols during visits to cleared facilities or change members of a visiting delegation at the last minute
- Foreign company seeks to establish joint ventures with cleared companies to act as U.S. company's representative in foreign markets
- Foreign company attempts to use a subsidiary in a third country to establish business relationships or buy interests in a cleared U.S. company
- Foreign company targets U.S. cleared employees, or those working in support of cleared companies for information beyond the scope of the current relationship

EXPLOITATION OF BUSINESS ACTIVITIES

“China uses foreign ownership restrictions, such as joint venture requirements and foreign equity limitations, and various administrative review and licensing processes, to require or pressure technology transfer from U.S. companies.”

Annual Intellectual Property Report to Congress, February 2019

WHAT IS TARGETING DURING CONFERENCES, CONVENTIONS, OR TRADESHOWS?

Conferences, conventions, or tradeshows host a wide array of presenters, vendors, and attendees. This provides a permissive environment for foreign collectors, commercial rivals, start-up companies, IOs, opportunists, and organized criminals to question vendors, develop business/social relationships, access actual or mockups of targeted technology, and interact with SMEs.

In 2019, nine percent of cleared industry reporting of suspicious contact-related activities occurred during attendance at conferences, conventions, or trade shows.

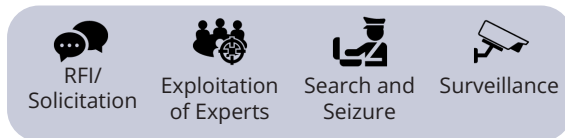
WHO IS BEING TARGETED?

Foreign collectors target anyone with access to targeted information and technology, or any SME in sought-after research or technology.

WHAT IS BEING TARGETED?

- Information, technical specifications, DoD plans, budgets/costs, system locations, and system pictures displayed at booths
- Information about cleared and uncleared employees to determine location to information, vulnerability to recruitment, and personnel interests to be used as pretext for future contact
- Physical or virtual access to company equipment
- Proprietary formulas and processes
- Blueprints and prototypes
- Research
- Vendor information
- Software information, i.e. source codes
- Company information – phone directories, corporate financial data, investment data, budgets, acquisitions, and sales

HOW ARE YOU BEING TARGETED?



FIEs pose as potential customers, attendees, exhibitors, scientists, or as representatives of a nation other than their own.

Collectors attempt to elicit CUI and classified information through casual conversation during and after official events.

FIEs use these occasions to spot and assess individuals for potential recruitment. They use charm and/or potential business incentives to soften their targets.

During foreign travel, security personnel can subject attendees to search and seizure of documents and electronic devices, as well as surveillance at the venue, while socializing, and while in hotels.

HOW CAN YOU RECOGNIZE IT?

At conferences, conventions, or tradeshows you may witness:

- Attempts to steal actual or mockups of technologies on display
- Photography of displays, especially when photography is explicitly prohibited



- Requests for information beyond the conference's scope
- Requests for the same information from different people during the conference
- Attempts to schedule post-event meetings or contact and attempts to develop personal friendships
- Attempts to contact you before, during, or after the meeting by phone, email, or social media

While traveling to and attending events, traditional IOs will use the following techniques to obtain information about you, your work, and your colleagues:

- Detailed and probing questions about specific technology
- Overt questions about CUI or classified information
- Casual questions regarding personal information collectors can use to target them later
- Prompting employees to discuss duties, access, or clearance level
- Attempts to access your electronic devices, i.e., laptop, smartphones
- Attendees not wearing IDs/name tags or wearing them incorrectly

COUNTERMEASURES

- Display signage requesting no touching or photography of items on display
- Complete annual CI awareness training
- Attend security briefings and de-briefings
- Remain cognizant of your surroundings and anyone

displaying increased interest in you or your exhibit

- At events, display mockups, not actual working versions of your product
- Do not leave technology, mockups, sensitive documents, or electronics unattended
- Create controlled access areas for sensitive displays that should not be touched or photographed
- Prepare responses for questions involving CUI or classified aspects of your product
- If your company provides WiFi for employees, create a strong password, and change it before and after each show

WHEN ATTENDING EVENTS OVERSEAS

- Request a threat assessment from the program office and your local DCSA representative prior to traveling to an event overseas
- Use designated travel laptops that contain no CUI or exploitable information
- Do not use foreign computers or fax machines and limit sensitive discussions
- Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return
- Do not post pictures or mention you are on travel on social media
- Do not accept electronic gifts

TARGETING DURING CONFERENCES, CONVENTIONS, OR TRADESHOWS

Immediately notify your FSO if you observe any of the following behaviors or believe you were targeted by an individual attempting to obtain information or technology they are not authorized to have:

- Offers to act as a foreign sales agent
- Attempts to steer conversations toward job duties or access to sensitive information or technology
- Insistent questioning outside the scope of what you are cleared to discuss
- Excessive photography/sketches, especially in areas that prohibit photography
- Individuals returning to the same booth multiple times to speak with different cleared employees
- Strangers trying to establish personal relationships outside work parameters
- Unusual or suspicious attempts at ongoing contact, including sending a follow-up email upon your return to the office
- Multiple individuals simultaneously asking questions, attempting to get you to reveal more than you should
- Theft of or missing items from your booth/display

WHAT TO REPORT

PREPARING FOR FOREIGN VISITORS

Foreign visitors are common in today's global economy. CCs should be aware of potential CI vulnerabilities and threats. While most visitors are here for legitimate purposes, the sheer volume of visitors makes it difficult to detect those with ulterior motives.

Foreign delegation visits to CC facilities are one of the most frequently used methods to target and attempt to gain access to CUI from cleared industry.

WHY DO FOREIGN ENTITIES TARGET U.S. CLEARED INDUSTRY?



It is cheaper for foreign entities to illicitly obtain CUI or classified information and technology than to fund initial R&D themselves. The U.S. Government spends more on R&D than any other country in the world, making U.S. contractors performing R&D prime targets for foreign collection of classified and unclassified commercial technology.

When a foreign visit occurs at your facility, preparation and awareness are essential to preventing loss of information. Stay alert and watch for indicators to help assess the potential for visitor targeting or collection.

HOW ARE YOU BEING TARGETED?

- **Peppering:** Visitors ask a variation of the same question or one visitor asks the same question to multiple employees
- **Wandering Visitor:** The visitor uses the distraction provided by a large delegation to slip away, out of the escort's control. Once away from the escort, the visitor may try to access a restricted area, sensitive or classified documents, or unattended and unlocked information systems
- **Divide and Conquer:** Visitors corner an escort away from the group and attempt to discuss unapproved topics to remove the escort's safety net of assistance in answering questions
- **Switch Visitors:** Delegations may add a new visitor to the group at the last minute, leaving little or no time for the company to vet the new visitor against known IOs
- **Bait and Switch:** The visitors plan to discuss one business topic, but after arriving, they attempt to discuss the CCs other projects, often dealing with CUI or classified information
- **Distraught Visitor:** When the visitor's questions are not answered, he/she acts insulted or creates an uncomfortable scene to psychologically coerce information from the target
- **Use of Prohibited Electronics:** The visitors bring unauthorized electronic devices such as cell phones, cameras, or thumb drives into restricted space

COUNTERMEASURES*

- Conduct a pre-visit facility walkthrough to ensure visitors cannot hear or see CUI, export-controlled information, or classified information during their visit
- Vet incoming foreign visitors with your supporting DCSA CI special agent
- Prior to the visit, brief all escorts and personnel working with the delegation on what they can and cannot discuss
- Develop standard, acceptable responses to questions that may arise, especially if projects are CUI or classified, are not applicable to the country visit, or include proprietary information
- Ensure there are enough escorts to properly support the number of visitors and escorts know where in the facility visitors can and cannot access
- Train escorts to detect suspicious behavior and questions, ensure they know to maintain visual contact with all visitors at all times, and develop contingency plans to handle visitors who leave the group
- If the delegation attempts to make additional contacts with escorts and speakers, ensure they limit discussions to the agreed-upon topics and information
- After the visit, debrief the host and all escorts to uncover if visitors exhibited any strange or suspicious activities or asked unusual and probing questions

**For additional information, see Code of Federal Regulation (CFR) 32 Part 117 National Industrial Security Program Operating Manual (NISPOM).*

LONG-TERM VISITS AND JOINT VENTURES

Long-term visits or joint ventures may provide an opportunity for a foreign long-term visitor to obtain restricted/proprietary information. They also provide an opportunity for visitors to spot, assess, and befriend employees that may assist, wittingly or unwittingly, in collecting restricted/proprietary information.

WHAT TO REPORT

View as suspicious any line of questioning concerning military or intelligence-based contracts or dual-use technology, unless topics were previously approved.

Even if an appropriate authority grants a foreign visitor access to classified U.S. information, that visitor is not entitled to classified information unless he/she has cleared need-to-know that has been communicated and verified in advance of the visit.

Inform your DCSA Industrial Security Representative or DCSA CI Special Agent of proposed foreign visitors. Given adequate time, they can assist with identifying risks to the cleared company, its technology, and its personnel.

View as suspicious any attendee's effort to contact you before, during, or after the visit by phone, email, or social media.

If any suspicious incidents occur during the visit, report them to your FSO immediately.

PREPARING FOR FOREIGN VISITORS



WHAT IS EXPLOITATION OF GLOBAL SUPPLY CHAINS?

Exploitation of the global supply chain refers to FIE attempts to compromise a supply chain.

A supply chain is a network of suppliers, manufacturers, developers, warehouses, distribution centers, transportation, outlets, and personnel. The supply chain may be global.

Organizations should protect against supply chain threats by employing a standardized process to address supply chain risk as part of a comprehensive information security strategy.

WHO IS BEING TARGETED?

- Design, Manufacturing, and Assembly Personnel
- Technicians
- Software Developers
- Stock Control Specialists

HOW ARE YOU BEING TARGETED?

Supply chain exploitation includes introducing counterfeit or malicious products or materials into the supply chain to:

- Gain unauthorized access to protected data
- Alter data
- Disrupt operations
- Interrupt communication

- Reverse engineer
- Cause disruption to design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an entity
- Intercept, disrupt, or delay shipping

METHODS OF OPERATION



METHODS OF CONTACT

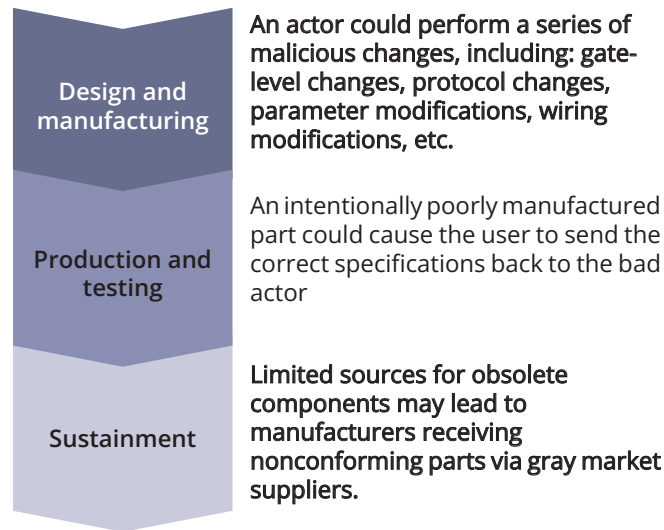


HOW CAN YOU RECOGNIZE IT?

- A device that exhibits functionality outside its original design
- Employees violating security protocols for handling components or introducing non-compliant components
- Dealers offering rare or obsolete components at low prices
- Dealers offering short lead times for large component orders
- A device or multiple devices from a lot exhibiting a unique error or failure
- Shipping containers showing signs of tampering

WHY IS IT EFFECTIVE?

- Successful exploitation of supply chain enables foreign agents to manipulate DoD system components, degrading capabilities and effectiveness or enabling access to CUI
- Counterfeit components will not perform to specification and can include malicious logic intended to degrade or destroy DoD systems and cause poor system interoperability, injury, loss of life, or compromise of national security
- Nonconforming parts are difficult to identify
- An actor with insider access could introduce malicious changes during any phase:



COUNTERMEASURES

TO MITIGATE TAMPERING WITH COMPONENTS AT CLEARED FACILITIES:



TO MITIGATE THREAT OF COUNTERFEIT COMPONENTS:

- Vet 2-3 levels down the supply chain
 - Use available all-source intelligence analysis to plan acquisition strategies/tools/methods
 - Integrate acquisition offices with other departments, including information assurance and security offices
 - Ensure subcontractor/off-site production facilities conduct effective supply chain risk management
 - Create incentives for suppliers who: implement required security safeguards, promote transparency into organizational process and security practices, provide additional sub-supplier vetting, restrict purchases from specific suppliers, and provide contract language that prohibits compromised or counterfeit components
 - Always use independent verification and validation for obsolete microelectronics and to vet external testing houses
 - Consider lifetime buys for components; avoid purchasing gray market, nonconforming parts
- Validate vendor with DoD customers/other authorized resources prior to purchase

EXPLOITATION OF GLOBAL SUPPLY CHAINS

WHAT TO REPORT

A suspicious contact occurs when someone attempts to introduce counterfeit or malicious products or materials into the supply chain.

EXAMPLES OF REPORTABLE ACTIVITIES

- Inadvertently or deliberately attempting to break a trusted chain of custody
- Introducing counterfeit components into a U.S. Government system during production
- Unauthorized personnel, of any nationality, attempting to access restricted areas of a cleared facility involved in producing components for DoD systems
- Any individual, regardless of nationality, attempting to compromise a cleared employee involved in manufacturing, assembling, or maintaining DoD systems
- Devices exhibiting functionality outside the original design
- A device, or multiple devices from a lot, exhibiting a unique error or failure

WHAT IS THE THREAT POSED BY EXPERT NETWORK COMPANIES?

- Expert Network Companies (ENCs) (a.k.a Knowledge Brokers) connect SMEs with researchers, investors, or businesses seeking specialized insights and advice on industries, markets, or technical areas. These clients pay a premium to connect with experts who provide advice not otherwise available.
- ENCs act as a bridge between clients and experts, establishing a periodic, recurring, or continuous relationship. ENCs are used by organizations seeking to gain knowledge quickly and make informed decisions.

WHO IS BEING TARGETED?



SMEs including cleared contractors, DoD service members, and former service members

WHAT IS BEING TARGETED?

- Electronics
- Optics and Lasers
- Radars
- Emerging Technology
- Space Systems
- Marine Systems
- C4
- Non-public Information on U.S. Government Policy

WHAT IS VALUABLE TO FOREIGN ADVERSARIES?

- Foreign governments aren't just interested in classified or export restricted information. Proprietary practices, supply sources, composition of materials, business methods, financial plans, or data handling are common requests through ENCs, some of whom are based in the United States.

"Foreign adversaries are leveraging LinkedIn in attempts to recruit both current and former Department of Defense (DOD) members, masquerading under the pretext of consulting, in a bid to gain strategic advantages in the great power competition."

Lt Col Lisenbee, Journal of Indo-Pacific Affairs, Air University, USAF

HOW ARE YOU BEING TARGETED?

- ENCs offer CCs, DoD service members, and former service members the opportunity to provide consultation for lucrative payment.
- ENCs connect the expert to undisclosed third parties, some being foreign individuals and organizations. Experts report being unable to ascertain the client's identity.
- While most ENC solicitations involve legitimate purposes, the nature of the process allows individuals or organizations to target technology and information while maintaining relative anonymity.
- Concealing the client's identity and keeping communications confidential creates an attractive environment for a FIE. This poses a security vulnerability and allows a foreign adversary to take advantage of the purview provided by ENCs, obtaining information while maintaining anonymity.

HOW ARE EXPERTS FOUND?

- Professional networks
- Social media platforms
- Industry events and conferences
- Academic affiliation
- Referrals
- Publicly published material
- Experts seeking opportunities

HOW ARE EXPERTS CONTACTED?

- Social Media Requests
- Email
- Telephone Call
- Professional Networking
- Sites
- Industry Events

HOW CAN YOU RECOGNIZE IT?

POTENTIAL INDICATORS OF FIEs

- Exceptionally high rates of pay per hour; payments in cryptocurrency or gift cards
- Offers to travel outside the United States
- Requesting information about a specific foreign government
- Requests to provide classified, controlled, or proprietary technology
- Requests for material support
- Bait and switch: requesting one topic, then changing to another
- Switching platforms outside the ENC
- Requests for personal information

COMMON FIELDS EMPLOYING ENCs

- Investment, Insurance, and Financial Services
- Medical Fields
- Electronics
- Manufacturing
- Security
- Government and Politics
- Business Strategy
- Aerospace Engineering
- Policy Development
- Economics

EXPERT NETWORK COMPANIES

WHY DO COLLECTORS USE THIS METHOD?

It is cheaper for FIEs to illicitly obtain CUI or classified information and technology than to fund the initial R&D themselves. The U.S. Government spends more on R&D than any other country in the world, making U.S. contractors performing R&D prime targets for foreign collection of classified and unclassified commercial technology.

VIGNETTE

A foreign company requests a wind tunnel modeling expert through an ENC and offers to pay them \$X per hour. A professor specializing in wind tunnel modeling receives the solicitation, accepts the offer, and virtually meets with Company A for several hours, assisting them in managing the data. The expert is paid for their time and Company A can reach back out to that expert in the future for more assistance, establishing a working relationship.

WHAT IS THE IMPACT OF LOST TECHNOLOGY?

The IP Commission 2021 review stated:
“IP-intensive industries support more than 45 million U.S. jobs. IP theft costs the U.S. economy hundreds of billions of dollars annually and reduces U.S. companies’ research and development (R&D) investment and innovation.”

Lost intellectual property harms national security and the U.S. economy.

NATIONAL SECURITY IMPACT

Leading-edge technology is vital to national security in intelligence and defense sectors.

- Technological advantage is vital to success on the battlefield
- Adversaries that mitigate U.S. systems’ effectiveness or deploy equal capabilities on the battlefield will cost U.S. and allied warfighter lives
- Adversaries with equal C4ISR capabilities may gain information superiority over U.S. and allied forces

ECONOMIC IMPACT

The IP Commission estimated counterfeit goods, pirated software, and trade secret theft, including cyber-enabled trade secrets, directly cost the U.S. economy \$225 to \$600 billion annually, or 1 to 3 percent of gross domestic product in 2016.

- Innovation is vital for commercial success; R&D requires investment of resources
- R&D investment includes the risk the product or process will not be commercially successful
- Foreign competitors can save on expense and risk involved in R&D by targeting IP at U.S. companies
- IP and technology lost to foreign competitors costs U.S. companies market share overseas and may lead to counterfeit products entering U.S. markets
- Lost revenue may impact funding for further R&D and the company can fall behind foreign and domestic competitors
- Revenue lost to foreign competitors illicitly producing a U.S. company’s product hurts the company’s profitability/ fiscal viability
- Eventually, revenue lost to counterfeit goods, pirated software, and lost IP will cost jobs at U.S. companies

WHO IS BEING TARGETED?

Foreign collectors target anyone with access to targeted information and knowledge of information system or security procedures:

- Developers
- Technicians
- Supply Chain Personnel
- Information Systems Personnel
- Business Development Personnel
- Human Resources (HR) Personnel
- Foreign Access Points
- Senior Managers
- SMEs
- Administrative Staff

WHY TARGET U.S. CLEARED INDUSTRY?

It is cheaper for foreign entities to illicitly obtain CUI or classified information and technology than to fund initial R&D themselves.

The U.S. Government spends more on R&D than any other country in the world, making U.S. contractors performing R&D a prime target for foreign collection of classified and unclassified commercial technology.

HOW ARE YOU BEING TARGETED?



Exploitation of Business Activities

- Joint ventures providing access to proprietary information
- Forced technology transfer when conducting business overseas



Academic Solicitation

- Submitting résumés for academic and research positions
- Reviewing academic papers
- Inviting researchers to present at conferences or for academic collaboration



Exploitation of Cyber Operations

- Malicious code injection
- Brute force attack
- Credential harvesting



Acquisition of Technology

- Purchasing systems to gain underlying components/ software
- Reverse engineering systems, components, and coding



Insider Threat

- Trusted personnel with legitimate access stealing information

“We see Chinese companies stealing American intellectual property to avoid the hard slog of innovation and then using it to compete against the very American companies they victimized—in effect, cheating twice over.”

Christopher Wray, Director
Federal Bureau of Investigation

IMPACT OF LOST TECHNOLOGY



COUNTERMEASURES






- Adhere to facility information, personnel, physical, and information system security policies
- Be aware of suspicious activities that might indicate attempts to illicitly obtain information from your company
- Report suspicious activities to the FSO



WHAT ARE METHODS OF OPERATION AND METHODS OF CONTACT?

- **MOs:** Distinct patterns or methods of procedure thought to be characteristic of or habitually followed by an individual or organization involved in intelligence activity
- **MCs:** Approaches used to connect the foreign actor to the targeted individual, information, network, or technology in order for the foreign actor to execute the MO

METHODS OF OPERATION

-  **Attempted Acquisition of Technology**
Acquiring protected information in the form of controlled technologies, via direct contact or through the use of front companies or intermediaries, including the equipment itself or diagrams, schematics, plans, spec sheets, or the like.
-  **Exploitation of Business Activities**
Establishing a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales, or service providers; leveraging an existing commercial relationship in order to obtain access to personnel or protected information and technology.

-  **Exploitation of Cyber Operations**
FIEs or other adversaries compromising the confidentiality, integrity, or availability of targeted networks, applications, credentials, or data with the intent to gain access to, manipulate, or exfiltrate personnel information or protected information and technology.
-  **Exploitation of Experts**
Gaining access to personnel or protected information and technology via requests for, or arrangement of, peer or scientific board review of academic papers or presentations; requesting a consult with faculty members or SMEs; or attempting to invite or otherwise entice SMEs to travel abroad or consult for foreign entities.
-  **Exploitation of Insider Access**
Trusted insiders exploiting their authorized P&A within cleared industry or causing other harm to compromise personnel or protected information and technology.
-  **Exploitation of Relationships**
Leveraging existing personal or authorized relationships to gain access to protected information.
-  **Exploitation of Security Protocols**
Visitors or unauthorized individuals circumventing or disregarding security procedures or behaviors by cleared or otherwise authorized persons that indicate a risk to personnel or protected information and technology.

-  **Exploitation of Supply Chain**
Compromising the supply chain, which may include the introduction of counterfeit or malicious products or materials into the supply chain with the intent to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communications.
-  **Résumé Submission**
Foreign persons submitting résumés for academic or professional placement that would facilitate access to protected information to enable technological or economic advancements by the foreign entity.
-  **RFI/Solicitation**
Collecting protected information by directly or indirectly asking or eliciting personnel or protected information and technology.
-  **Search/Seizure**
Temporarily accessing, taking, or permanently dispossessing someone of property or restricting freedom of movement via tampering or physical searches of persons, environs, or property.
-  **Surveillance**
Systematically observing equipment, facilities, sites, or personnel associated with contracts via visual, aural, electronic, photographic, or other means to identify vulnerabilities or collect information.
-  **Theft**
Acquiring protected information with no pretense or plausibility of legitimate acquisition.

METHODS OF CONTACT

- Conferences, Conventions, or Tradeshows**
Contact regarding or initiated during an event, such as a conference, convention, exhibition, or tradeshow.
- Cyber Operations**
Activities taken directly against a targeted system; to include cyber network attack, cyber network exploitation, and collection.
- Email**
Unsolicited requests received via email for information or purchase requests.
- Foreign Visit**
Activities or contact occurring before, during, or after a visit to a contractor's facility.
- Mail**
Contact initiated via mail or post.
- Personal Contact**
Person-to-person contact via any means where the foreign actor, agent, or co-optee is in direct or indirect contact with the target.
- Phishing Operation**
Emails with embedded malicious content or attachments for the purpose of compromising a network including spear-phishing, cloning, and whaling.

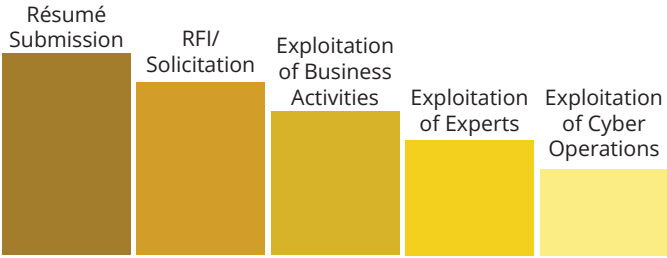
- Résumé - Academic**
Résumé or CV submission for academic purposes.
- Résumé - Professional**
Résumé or CV submissions for professional purposes (e.g. seeking a position with a cleared company).
- Social Networking Service**
Contact initiated via a social or professional networking platform.
- Telephone**
Contact initiated via a phone call by an unknown or unidentified entity.
- Web Form**
Contact initiated via a company-hosted web submission form.

WHAT IS THE VALUE OF MOs/MCs?

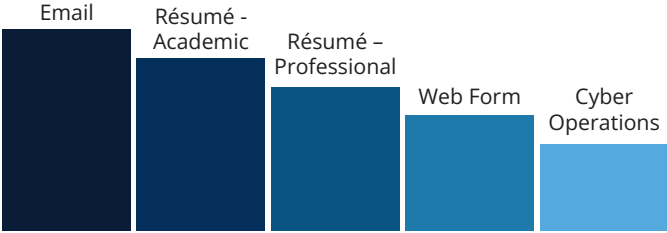
Knowing the methods used by FIEs and how they contact targeted personnel or facilities aids in the early identification of possible foreign targeting of technologies resident in cleared industry. This is vital in our efforts to identify, assess, and disrupt FIE threats to DCSA, the trusted workforce, and the cleared national industrial base.

METHODS OF OPERATION AND METHODS OF CONTACT

FY2023 MOST COMMONLY REPORTED METHODS OF OPERATION



METHODS OF CONTACT



REPORTING REQUIREMENTS

Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM) requires reporting suspicious contacts, behaviors, and activities.

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting CI threats and mitigating risks.

DCSA: <https://dcsa.mil>

DCSA, Office of Counterintelligence: <https://www.dcsa.mil/mc/ci>

Center of Development of Security Excellence: <https://www.cdse.edu>