COUNTERINTELLIGENCE

Best Practices for Cleared Industry

COUNTERINTELLIGENCE AWARENESS & REPORTING

WHAT IS THE THREAT?

Our Nation's secrets and technological advantages are in jeopardy–the same secrets that make your company profitable. U.S. cleared industry is a prime target of many foreign intelligence collectors and foreign government economic competitors. The nature and extent of industry threat reporting suggests a concerted effort to exploit cleared contractors for economic and military advantage. These contacts range from outright attempts to steal technology to seemingly innocuous business and/or academic ventures. Through analysis of industry reporting, DCSA has found that foreign intelligence services use both commercial and government-affiliated entities. The large number of commercial contacts likely represents foreign governments' attempts to make contacts seem more innocuous by using non-threatening approaches.

WHO ARE THEY TARGETING?

ANYONE WITH ACCESS TO NATIONAL DEFENSE INFORMATION

Foreign collectors may target anyone with access to the targeted information, knowledge of information systems, or security procedures, including:

Developers: Scientists, researchers, engineers, and program managers who research and develop leading technologies

Technicians: Engineers/specialists who operate, test, maintain, or repair targeted technologies

Supply Chain Personnel: Personnel involved in sourcing and purchasing components integrated with a deliverable defense product or technology, including stockroom control specialists

Information Systems Personnel: Systems administrators or others with 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: HR representatives with 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): Scientists and engineers involved with targeted technology publishing in technical journals, participating in professional associations and/or academia, and patent owners

Administrative Staff: Secretaries, administrative/executive assistants with access to leadership calendars, contact lists, and company proprietary information

MOST COMMON COLLECTION METHODS

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, product specification sheets, or the like. Contact methods often involve email, mail, cold-calling employees, web card submissions, contacts at trade shows, foreign sales representatives, or use of a website's "Contact Us" application.

Indicators of Suspicious Purchase Requests:

- The customer or address is similar to one listed on the Commerce Department's Denied Persons List, the Entity List, or other government suspicious entities lists
- Suspicious delivery addresses such as an obscure P.O. Box, residence, or multiple businesses using the same address
- Customer is reluctant to offer information about the end-use of the item
- Customer's line of business does not fit product's applications
- The customer wants to pay cash for a very expensive item when the sale terms would normally call for financing
- The customer has little to no business background available
- The customer declines routine installation, training, or maintenance/warranty services
- The customer is unfamiliar with the product's performance characteristics but still wants the product
- The customer uses third-party broker or address is listed in a third country
- Solicitor acts as a procurement agent for a foreign government
- The customer requests commercial technology modified for military use

Exploitation of Business Activities:

Establishing a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales, or service provider; and leveraging an existing commercial relationship in order to obtain access to controlled unclassified information (CUI) in the form of 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. Contact methods often 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 directly or indirectly asking or eliciting personnel for protected information and technology.

Common Methods of Contact for RFI:

- Conferences, conventions, and tradeshows
- Email, surveys, telephone, web forms
- Foreign contacts, visits, and travel

Exploitation of Insiders:

Trusted insiders exploiting their authorized placement and access within cleared industry or causing other harm to compromise personnel or protected information and technology.

Exploitation of Experts:

Gaining access in order to obtain access to CUI in the form of personnel or protected information and technology. Contact methods may include soliciting SME participation in foreign conferences, such as paper submissions, invited speaker, or technical board positions; or offering SMEs foreign academic faculty positions and paid offers to collaborate with foreign academic institutions.

Exploitation of Cyber Operation Methods:

Foreign intelligence entities 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. Cyberspace exploitation continues to be a key concern. The potential for blended operations where cyber activity contributes to theft presents a great risk to cleared industry.

COMMON CYBER OPERATION METHODS

- **Phishing Operations:** Emails with embedded malicious content or attachments for the purpose of compromising a network to include, but not limited to, spear phishing, cloning, and whaling
- **Watering Hole:** Use of a compromised website to target visitors. These could be third-party websites or your company website to access your customers or persons with common interests
- **Patch Management:** Attacks that exploit outdated networking equipment and unpatched software/hardware vulnerabilities
- **Exploitation of Mobile Devices:** Tampering with mobile devices that have trusted access to a protected network
- **Introduction of Backdoor Access Panels**

TRAINING REQUIREMENTS

Cleared contractors are required to receive training on Threat Awareness, Counterintelligence (CI) Awareness, and reporting requirements as per the National Industrial Security Program Operation Manual (NISPOM).

ELICITATION

WHAT IS ELICITATION?

Elicitation is a structured method of communication used to extract predetermined information from people without making them aware that they are a collection target.

Elicitation comes in many forms. Communications can be verbal or written. The elicitor has specific goals for the exchange and the target is unaware that the elicitor is attempting to collect sensitive or classified information from them.

Setting is important in elicitation. Often the elicitor will attempt to conduct their collection activities away from the target's work. This helps the target relax and can make them less security conscious, as well as introduce other factors that can ease the elicitation process, such as alcohol.

Because elicitation can sound like a common conversation, it can be difficult to tell whether it is an innocent, friendly conversation, or intelligence gathering. Foreign intelligence entities look for anything from details about programs you or your colleagues work on to personal information they can use in future targeting efforts.

Elicitation requires patience and persistence. Pieces of information, collected over an extended period, can provide the information the elicitor required. The aggregate of information, even unclassified information collected over an extended period of time, could give the adversary the desired information about technology, programs, and processes.

ELICITATION METHODS OF OPERATION

• **Exploitation of Tendency to Complain:** Statements such as "Boy I am so behind at work" can elicit a cleared employee's response that would divulge 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 a few questions they want answered with other logical questions. Or merely uses a survey to get people to agree to talk to you.

• **Feigning Ignorance:** An elicitor can portray ignorance to have the target "teach" or instruct them about a topic. This tactic is frequently employed in academia. This exploits the habit of teaching or lecturing and can put the academic into a familiar frame of mind to share information.

• **False Statement:** An elicitor can knowingly make a false statement so the target can correct them. This is often a modification of criticism. Another way to use false statement is to cite someone else's research or paper. This can be particularly effective if the target knows about the area of study or research.

• **Flattery:** Cleared contractor employees provide a valuable service to America. They should be proud of the work they do. Flattery can elicit numerous responses such as bragging about work, or a tendency to give them credit for work, but either way the target is having conversations about topics of interest. Flattery can start as simple as "Boy that thing is really cool."

• **Quid Pro Quo or Trading Confidences:** In quid pro quo, the elicitor provides the target with valuable information. Quid pro quo can start with, "I shouldn't tell you this but" or "This is off the record." The purpose is to make the target feel obligated to return the favor and provide valuable information to the elicitor. Espionage may look more like a business transaction and less like gathering information.

• **The Paper Review:** Many cleared employees have ties to academia and research institutions. Cleared employees regularly receive requests to peer review research or academic theses. Many of these requests are harmless and straightforward, but some are attempts to have cleared employees leverage their sensitive or classified research to correct or expand on research in topics similar to their work.

• **Bracketing:** Bracketing occurs when the elicitor asks a target about a sensitive value using a high and low value rather than asking for a specific number. This could be a range within a system, such as the elicitor asking if the range is somewhere between 10 and 15 kilometers. This could garner a response such as "Yes, in the high end" or "Well, a little more than that." Bracketing allows the elicitor to adjust their bracket for their next target.

• **Oblique Reference or Analogies:** In this method, the elicitor discusses a topic similar to the target's work so the target will use their own work to make a point of reference. An example would be the elicitor discussing a foreign or civilian system similar to the target's work. The target is likely knowledgeable of and comfortable discussing this topic. On the finer points of the discussion the target may slip and use their own sensitive system as a point of reference to the foreign system.

• **Criticism:** Criticism can be accomplished by seemingly inadvertently criticizing the target or knowingly criticizing the target. An example would be 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 vehemently defend the things they feel passionate about.

HUMAN FACTORS THAT ENABLE ELICITATION:

• Desire to seem polite and helpful, even to strangers

• Desire to seem knowledgeable or well informed

• Desire to seem competent

• Desire to feel appreciated and believe we are contributing to something important

• Tendency to gossip

• Tendency to correct others

• Tendency to underestimate the information's value

• Tendency to believe others are honest

• Tendency to complain

• Tendency to show empathy toward others

• Tendency to be indiscrete, especially when emotionally charged

DEFLECTING ELICITATION ATTEMPTS

In the event you are targeted, 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, your family, or your co-workers. If you believe someone is attempting to elicit information from you, you can:

• Change the topic

• Refer them to public websites

• Deflect question with one of your own

• Provide a vague answer

• Explain that you don't know, and respond with "Why do you ask?"

• Take control of the conversation

• Casually request to take a photo with them, to remember "your most important prospects"

• Consider: If you have to say "No" let your facility security officer (FSO) know

WHAT TO REPORT

Elicitation is a "suspicious contact" reportable by cleared companies to the Defense Counterintelligence and Security Agency (DCSA) under the National Industrial Security Program (NISP). Examples of reportable activity include:

• 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, you should report any suspicious conversations to your FSO, DCSA Industrial Security Representative, and DCSA Counterintelligence (CI) Special Agent. These individuals can assess your information and determine whether a potential CI concern exists

PERSONAL CONTACT

DEFINING PERSONAL CONTACT

Person-to-person contact occurs by any means where the foreign actor, agent, or recruiter is in direct or indirect contact with the target.

Foreign intelligence entities (FIE) commonly use a method and technique called elicitation to collect intelligence through what appears as normal, even mundane, social or professional contact. An FIE method of operation attempts to confirm or expand their knowledge of a sensitive program or gain clearer insight into a person's placement and access (P&A) prior to possible recruitment.

PRIMARY METHODS OF OPERATION AND EXPLOITATION

This method of contact is associated with all methods of operation FIE apply when targeting cleared industry. Those with the highest risk include:

- Exploitation of Commercial/Business Activities
- Exploitation of Insider Access
- Exploitation of Security Protocols
- Request for Information

(RFI)/Solicitation

- Exploitation of Relationships
- Search/Seizure

WHO ARE THEY TARGETING?

YOU are at risk simply because YOU have access to classified or sensitive intelligence. FIE aggressive collectors will target anyone with P&A to obtain desired information, knowledge of information systems, or awareness of security procedures.

This includes but is not limited to:

- ***Developers:*** Scientists, researchers, and engineers researching and applying new materials or methods to Department of Defense (DOD) programs and other leading-edge technologies.
- ***Technicians***: Engineers or specialists that operate, test, maintain, or repair targeted technologies
- ***Production Personnel:*** Personnel with P&A to targeted technologies' production lines or supply chains
- ***IT Personnel:*** Systems administrators or others with access to targeted facility networks and knowledge of network security protocols
- ***Business Development Personnel:*** Marketing and sales representatives, business travelers
- ***Human Resources Personnel:*** HR representatives with access to personnel records and job applicants
- ***Facility Employees:*** Anyone with P&A to a cleared or sensitive facility containing targeted information, including security, clerical, maintenance, and janitorial personnel

HOW CAN YOU RECOGNIZE IT?

This approach, by trained professional intelligence officers (IO) and non-traditional collectors, will usually be subtle.

Some likely indicators of this method include:

- Business contact requesting information outside the contract scope, or through an increased or gradual progression of information initiated from legitimately authorized business discussions
- 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 IOs are professionally trained in elicitation tactics and operate without borders. IOs focus on collecting protected and valuable information. Non-traditional collectors, such as business and academic contacts, leverage existing relationships to obtain restricted information outside the relationship scope. Because of this, not all elicitation attempts are obvious. They operate along a spectrum of least intrusive to most intrusive means.

The trained IO elicitor and non-traditional collectors will try to exploit natural human tendencies, including the desire or tendency to:

- Be polite and helpful, even to strangers or new acquaintances
- Appear well-informed, especially about your profession
- Expand discussion on a topic, likely giving praise or encouragement, to show off
- Correct others' comments
- Underestimate the value of the information being sought or given, especially if we are unfamiliar with how that information could be used
- Believe others are honest, a reluctance to be suspicious of others

COUNTERMEASURES

In the event you believe a personal contact has requested 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, your family, or your 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 feel uncomfortable.

If you believe someone is attempting to elicit information from you, you can:

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

Consider: if you have to say "No" let your facility security officer know.

WHAT TO REPORT

Personal contact is the vector for many intelligence methods of operation that constitute "suspicious contact." Report any instance where you suspect you may be the target 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 the 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, you should report any suspicious conversations to your facility security officer or Defense Counterintelligence and Security Agency (DCSA) Counterintelligence (CI) representative.

ACADEMIC SOLICITATION

WHAT IS ACADEMIC SOLICITATION?

DCSA defines academic solicitation as the use of students, professors, scientists, or researchers as collectors improperly attempting to obtain sensitive or classified information.

Placing academics at, and requesting to collaborate with, U.S. research institutions under the guise of legitimate research in order to access developing technologies and cutting edge research.

These attempts can include requests for, or arrangement of, peer or scientific board reviews of academic papers or presentations; requests to study or consult with faculty members; and requests for and access to 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 continues to rise, and the academic community will likely remain a top target for the foreseeable future.

Although most academic contacts are likely legitimate, some foreign academics may ultimately take advantage of their placement and access to further their country's research and development goals.

WHO ARE THEY TARGETING?

- Researchers, scientists, and subject matter experts conducting classified or controlled unclassified research/projects on behalf of a U.S. Government customer
- Researchers, scientists, and subject matter experts employed at cleared components of academic institutions or with unclassified and controlled unclassified information (CUI) work published in scientific or technical journals or presented at conferences
- Students, professors, and researchers with access to research and technical information (especially graduate and post-doctorate students)
- Researchers, scientists, and subject matter experts working on cutting-edge technology
- Subject matter experts teaching technical courses

> 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*

WHAT IS TARGETED?

- Classified, CUI, or export-restricted basic and applied research
- 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 the students, professors, and researchers working on the technologies

WHY DO COLLECTORS USE THIS METHOD?

- Academic solicitation is an effective way to collect information due to the academic community's collaborative nature
- Foreign countries can exploit their students' access to supplement intelligence collection efforts against emerging Department of Defense (DOD) and civilian technical research
- Sending students to study at U.S. academic and research facilities will provide better educated scientists and researchers for country-specific technology development

COUNTERMEASURES

- Be familiar with foreign intelligence entities methods or operation
- Know and understand the legal and institutional restrictions to the 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/facility security officer. 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 at higher echelons

EXAMPLES OF ACADEMIC SOLICITATION

- 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. subject matter expert review research papers, in hopes the expert will inadvertently provide information that assists with future research
- Request for a foreign exchange program or one-for-one swap

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 may include 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

> 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*

FOREIGN VETTING IN CLEARED ACADEMIA

RISK TO ACADEMIA:

United States academic institutions, specifically U.S. Government Affiliated Research Centers within academia persist as a target of non-traditional collection and acquisition of fundamental research and essential technology. Solicitation and collection of vital information via academia allows adversaries to identify dual-use technologies and transfer proprietary research. Foreign adversaries will continue to exploit the openness of U.S. academia and ongoing research as a means to transfer classified, unclassified, and controlled unclassified information, as well as sensitive and often export-controlled research to advance their national security interests. Proper vetting of foreign students, foreign faculty, as well as visiting foreign researchers and scholars is essential to protecting the vital research and development that occurs within U.S. academic institutions. Enhanced vetting efforts will play a vital role in thwarting adversarial acquisition, whether witting or unwitting, of essential research conducted at U.S. academic institutions. This job aid will educate and assist cleared academia on the 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 (patents, copyrights, royalties)
- Loss of endowments, gifts, donations, prestige, or loss of credit
- Loss of grants and contracts
- Regulatory fines, penalties, and criminal liabilities

INDIVIDUALS TO BE VETTED:

Non-immigrant students and visiting scholars associated with:

- Foreign military research and/or institutions
- Foreign government sponsorship (i.e. China Scholarship Council)
- Foreign government and/or military employment
- Scholarship requirements mandating internships with defense companies and/or contact with foreign diplomatic institutions
- Academic exchange agreements involving emerging and/or dual-use technology
- International cooperative programs for innovative talents and foreign influence (i.e. Thousand Talents, Foreign Experts Programs)
- Cultural Institutes (i.e. Confucius Institute)

VETTING BEST PRACTICES:

- 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. This list consolidates multiple export screening lists of the Departments of Commerce, State, and the Treasury. Any dealings with a party on any of these lists would violate U.S. export/sanctions regulations and would require further authorization and approval from the respective government agency:
    - **Denied Person List:** Individuals and entities that have been denied export privileges
    - **Unverified List:** End users who Department of Commerce's (DoC) Bureau of Industry and Security has been unable to verify in prior transactions
    - **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 that have been sanctioned under various statutes
    - **Arms Export Control Act** (AECA) **Debarred List:** Entities and individuals prohibited from participating directly or indirectly in the export of defense articles, including technical data and defense services
    - **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 there is a hit with respect to the screening of any individual or entity, contact your assigned DCSA CI Special Agent immediately.
- Leverage vetting support from supporting Federal agencies (DCSA, FBI, Military Services, NASA, DoE, DoC, etc.). Note: for non-U.S. persons only.
- Scrutinize Curriculum Vitae (CV), resumes, and applications for red flag issues:
    - False information
    - Links to denied party screening indicators (i.e. address, employment, references, etc.)
    - Similar or identical information with other applicants
    - Affiliations with foreign military research and/or institutions from high-threat countries
    - Research interest mismatches between applicant's declared interest and what reflects in the CV (i.e. applicant declared interest in a technology with a commercial/civil application but CV reflects a military application)
- Review applicant's research publications for red flag issues using web resources (Google Scholar, Research Gate, ORCID, Web Of Science, Dimensions)
    - Research topic conflicts between expressed interest and published work
    - Military related research topics and applications
    - Coauthors affiliated with high-threat countries and/or links to denied party indicators and institutions
- Verify applicant's references listed in the CV and/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 to include suspicious activity such as students not attending class, etc. This also 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, FBI, ICE and other federal law enforcement and security organizations for enhanced review and analysis of foreign applicant

REPORTING REQUIREMENT

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

If you suspect you/your company are targeted, report it immediately, which is critical to disrupting foreign intelligence threats and mitigating risks. Reporting allows us to share and address risks together. Report securely to your servicing DCSA CI Special Agent using encryption or DOD Safe.

EXPLOITATION OF INSIDER ACCESS

DEFINITIONS

Insider: Any person with authorized placement and access (P&A) to any U.S. Government or contract resource 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 that an insider will use their P&A, wittingly or unwittingly, 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.

WHY ARE NEFARIOUS ACTIVITIES EFFECTIVE?

Insiders have arguably caused more damage to United States security than foreign intelligence officers or cooptees, and with today's technological advances, insiders with P&A and intent to damage can cause more harm than ever before. Activities that previously took years to collect targeting information now take only minutes due to increased use of removable media.

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

HOW CAN YOU RECOGNIZE AN INSIDER THREAT?

Identifying potentially malicious behavior by employees with P&A to classified or controlled unclassified information (CUI) 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 made this personal decision because they did not acknowledge the insider threat patterns, or did not want to get involved or cause problems for their coworkers. Their failures to dutifully report caused grave issues for their company. Reporting insider threat is a requirement, not a choice.

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

Ignoring questionable behaviors can only increase the insider's potential damage to national security or threaten employee safety. While every insider threat's motives may differ, the CI indicators are generally consistent.

POTENTIAL ESPIONAGE OR RISK INDICATORS

• Repeated security violations or a general disregard for security rules

• Failure to report overseas travel or contact with foreign nationals

• Seeking to gain a higher security clearance or expand access outside job scope without need

• Engaging in classified conversations without a need to know

• Attempting to enter classified or restricted areas without authorization

• Working hours inconsistent with job assignment or unusual insistence on working in private

• Accessing information not needed for job

• Asking sensitive questions outside of "need to know" purview

• Foreign visitors wandering away from their escort at cleared contractor facilities

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

REPORTABLE BEHAVIORS

Information Collection:

• Keeping classified materials in an unauthorized location (e.g., at home)

• Attempting to access classified information without authorization

• Obtaining access to sensitive information inconsistent with present duty requirements

• Questionable downloads

• Unauthorized use of removable media

• Maintaining unauthorized backups

Information Transmittal:

• Using an unclassified medium to transmit classified material

• Discussing classified materials on a non-secure telephone or in non-secure emails or texts

• Removing classification markings from documents

• Unnecessarily copying classified material

Foreign Influence:

• Expressing loyalty to another country

• Concealing reportable foreign travel or contact

• Significant ties to family members in foreign countries

IMPACT

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

• Loss or compromise of classified or CUI

• Weapons systems cloned, destroyed, or re-engineered

• Loss of U.S. technological superiority

REPORTING

You are the first line of defense against insider threats. Help protect our national security by reporting any suspicious behavior that may relate to an insider threat.

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

Be aware of potential issues and actions of those around you and report suspicious behaviors and activities to your local security official/facility security officer.

CYBER THREATS

CYBER THREATS

Our nation's cyber adversaries have a plethora of tools and tricks from a multitude of resources, including publicly available information on the Internet. This access makes it increasingly difficult to differentiate between a criminal and an intelligence entity. This is exacerbated by the ease with which our adversaries can obtain information about potential targets. We live in a world where Internet of Things includes everything from computers, cell phones, Smart TVs, Alexa, Ring, watches, and even satellite radio, to refrigerators and window shades. Combine the two and the compounding problem becomes extreme and daunting. Sometimes the best solution is to go back to the basics and educate the workforce.

WHO ARE THEY TARGETING?

- Any organization or company, cleared or uncleared, with access to information coveted by our nation's adversaries
- Any individual, cleared or uncleared, regardless of job title or position, who can be used to gain access to an unsuspecting organization's network
- YOU and YOUR company

WHY ARE YOU A TARGET?

- Publicly available information (identifies people with placement and access)
- Contract information (bid, proposal, award, or strategies)
- Company website 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, public speaking engagements, and social networking sites such as Facebook and LinkedIn, etc.

WHAT ARE THEY TARGETING?

- International Traffic in Arms, export-controlled and critical technology, and controlled unclassified information (CUI)
- Research and development
- Company unclassified networks (internal and external), partner and community portals, commonly accessed websites, and unclassified search history
- Proprietary information (business strategy, financial, human resource, and product data)
- Administrative and user credentials (usernames, passwords, tokens, Virtual Private Network [VPN] data, etc.)
- Patch update sequences/patterns, i.e., is the company using a set date to update its systems?

Foreign intelligence entities seek the aggregate of CUI or proprietary documents which could paint a classified picture

HOW DO THEY COMPROMISE NETWORKS, SYSTEMS, AND TECHNICAL DATA?

- **Information Gathering:** Harvesting information (names, emails, relationships, publicly available vulnerabilities, and social engineering, etc.)
- **Targeting:** Coupling exploit with delivery method, such as email
- **Delivery:** Infecting the target commonly using email, website hijacking, and removable media (through insiders)
- **Exploitation:** Exploiting a vulnerability on a system to execute code
- **Installation:** Malware installation likely providing persistence on targeted network
- **Command and Control:** Communication avenue for adversary to remotely access a computer, network, or software/firmware
- **Actions on the Objective:** With access, the adversary can now access the targeted information, data, and technology

POTENTIAL COUNTERMEASURES

- Training! Training! Training!
- Using complex passwords
- Educating employees on social networking and email targeting; phishing email signs and reporting
- Defense in depth
- Technical defenses (firewalls, Domain Name System proxy, Internet content filtering, etc.)
- Patch management
- Monitoring suspicious network activity (even third-party vendors). Your network and your proprietary data are at stake
- Opening lines of communication among facility security, counterintelligence (CI), and network defense personnel–a one-sided defense is a failed defense
- 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

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 procedure to exfiltrate data and release to the public
- Supply Chain vulnerabilities
- Insecure Security Products (vulnerabilities)
- Malicious Code Injection
- Botnets
- Brute Force
- Social network sites
- Credential Harvesting

REPORTABLE TO DCSA

- All of the persistent and emerging cyber threats
- Aggressive port scanning outside normal network noise
- Advanced techniques and/or advanced 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, such as through social networking sites
- Unauthorized network access
- Actual or attempted unauthorized access into U.S. information systems
- Tampering with or introducing unauthorized elements into information systems
- Unexplained user accounts, administrator accounts, and expansion of network privileges
- Data exfiltration
- Malicious codes or blended threats such as viruses, worms, Trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration
- Unauthorized email traffic to foreign destinations
- Use of Department of Defense (DOD) account credentials by unauthorized parties
- Unexplained storage of encrypted data
- Network spillage incidents or information compromise
- Unauthorized transmissions of classified or CUI
- Any cyber activity linked to suspicious indicators provided by DCSA, or by any other cyber centers and government agencies

Foreign Intelligence Threat Via Social Media

FOREIGN INTELLIGENCE THREATS VIA SOCIAL NETWORKING SITES

Social networking sites (SNS) are everywhere in today's society. Worldwide SNS usage provides foreign intelligence entities (FIE) vast opportunities to exploit personnel, cleared or uncleared. The FIE goal is to obtain U.S. critical technology, proprietary data, advanced research and development, and many other aspects of valuable information in U.S. industry.

- 51% = Total world population; 3.96 billion people use social media
- 2.25 = Hours digital consumers spend daily on SNS and social messaging
- 79% = Number of adults in the United States that use at least one SNS
- 8.8 = Number of SNS accounts the average person maintains

Our Nation's foreign adversaries actively exploit SNS to serve their own malicious intentions. Once posted, information on SNS is no longer private and can never truly be deleted. The more information posted, the more vulnerable you may become. Using high privacy settings provides a layer of protection, although the information ultimately still resides on a server.

Loose lips sink ships. Everyone is a target when associated with cleared contract facilities, companies, technology, research and development, etc.

It is well known that SNS collect personal and trending information on account owners, which is used to tailor the individual's experience. Depending on the site, the information can be sold and companies can be hired to analyze user activities.

FIEs and foreign competitors use SNS to conduct collection activities:

- Request friend/professional connection
- Monitor social media accounts
- Elicit information
- Recruit assets

"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

METHODS OF OPERATION

Some methods of operation an adversary can use to conduct collection on SNS are techniques such as:

- Flattery
- Provide information to get information
- Find commonality
- High concentration of targeting on professional SNS
- Obfuscation of true identity – easy and cost effective
- Résumés can and have contained malware
- Detailed information makes an easy target for adversarial collectors
- Transition from SNS to real world using guise: recruiting, speaking engagements, etc

Fake personas on SNS:

- Realistic looking 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

Misinformation:

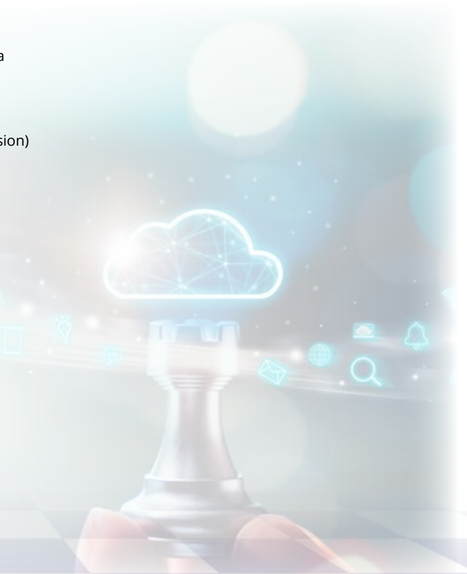
Adversaries can spread misleading or false information via SNS using fake bot accounts and troll farms. A troll farm is an organization whose employees or members attempt to create conflict and disruption in an online community. SNS uses algorithms that could inadvertently amplify the malicious content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

COUNTERING THE THREAT

- Think before you post
- Limit or exclude personally identifiable information
- Disable geotagging
- Consider a pseudonym
- Create strong passwords; change often
- Never put sensitive proprietary or controlled unclassified information on your SNS profile
- Be wary of unsolicited messages from unknown senders
- Do not accept connections from unknown sources
- Do not click/download anything
- 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 facility security office and the Defense Counterintelligence and Security Agency (DCSA)
- Make frequent updates to SNS configuration

WHAT TO REPORT

- Questionable or suspicious contacts on social media platforms
- Any 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 unintentionally downloaded
- Request for information, academic solicitation, job offers from adversarial countries
- Unsolicited contacts from unknown individuals



EXPLOITATION OF BUSINESS ACTIVITY

WHAT IS EXPLOITATION OF BUSINESS ACTIVITY?

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

WHO ARE THEY TARGETING?

• Any cleared employee or cleared company that supports cleared facilities, or that works with controlled unclassified information (CUI) or classified information relating to the Department of Defense (DOD) or other U.S. Government programs or systems

• Foreign collectors or their agents often target employees involved in business development, sales, marketing, information sharing, or other "professional collaborative efforts" to develop a relationship

• Once such an entity establishes a business relationship, they seek to leverage that relationship to contact other cleared employees working with targeted information and technology

WHY IS IT EFFECTIVE?

Foreign entities exploit legitimate activities with defense-oriented companies to obtain access to otherwise denied information, programs, technology, or associated U.S. personnel. This method of operation relies on the appearance of legitimacy provided by the established commercial or business activity. Conversely, U.S. company personnel, cleared or uncleared, seeking to build positive relationships and gain future business with foreign partners may unwittingly provide information beyond the scope of the business activity for which the relationship exists.

Examples of this exploitation 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 the U.S. company's network

• Foreign-produced hardware and software sold to a cleared company may include design vulnerabilities and malware that could provide foreign actors access to a company's networks and information

• Foreign collectors prey upon cleared employees' eagerness to develop or expand a commercial relationship 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 who are uninformed and uneducated on the commercial agreement's security limits or the technology's export control restrictions may commit a security violation by unwittingly providing information that should not be shared, based on the established relationship

WHAT ARE THE PRIMARY METHODS OF EXPLOITATION?

• Personal contact

• Cultural commonality

• Foreign visits

• Direct military sales

• Direct commercial sales

• Conferences, conventions, and tradeshows

• Cyber operations

• Email requests

• Business propositions and solicitations

• Academic solicitations

• Web form submissions

• Joint ventures

• Social networking sites

• Claiming to have been referenced by (XYZ), i.e., friend, another company/vendor/customer, etc

HOW CAN YOU RECOGNIZE IT?

A business relationship with a foreign company or person may be entirely legitimate. However, in many cases, foreign entities with nefarious motives and intent build relationships or abuse existing relationships with U.S. industry to establish pathways to restricted information and technology. Building on apparent 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 fora U.S. company

• Selling and installing hardware or software in cleared contractors' or sensitive facilities' networks

• Buying a substantial or majority interest in U.S. companies to gain intellectual property rights for technology, as well as to share data or appoint key management personnel in the acquired company

Potentially Suspicious Exploitation Scenarios:

• Foreign company has a nebulous business background

• Foreign company attempts to obscure ties to a foreign government

• Foreign company attempts to acquire interest in companies or facilities inconsistent with their 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 the 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, or offers partnership with the cleared company

"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

TARGETING DURING CONFERENCES, CONVENTIONS, AND TRADESHOWS

Foreign collectors, to include commercial rivals, start-up companies, intelligence officers, opportunists, and organized criminals, use many methods to gather information of value to foreign intelligence entities (FIE) to include current and emerging U.S. technology during conferences, conventions, and tradeshows.

They may pose as potential customers, attendees, exhibitors, or scientists, and even as representatives of a nation other than their own.

Collectors may attempt to directly ask about controlled unclassified information (CUI) or classified information or try to elicit information during casual conversation during and after official events.

In fiscal year 2019, nine percent of cleared industry reporting of suspicious contact related activities occurred during attendance at conferences, conventions, and tradeshows.

WHO ARE THEY TARGETING?

Foreign collectors will target anyone with access to the targeted information and technology, or any subject matter expert in sought-after research or technology.

WHAT ARE THEY TARGETING?

• Information, technical specifications, Department of Defense (DOD) plans, budgets/costs, system locations, and system pictures displayed at booths

• Information about cleared and uncleared employees to determine their location to information, vulnerability to recruitment, and personnel interests that could be used as a pretext for future contact

• Information about DOD plans, intentions, budgets/costs, and system locations

• Adversaries may try to gain physical or virtual access to company equipment

• Proprietary formulas and processes

• Blueprints and prototypes

• Research

• Vendor information – people with whom you conduct business/your supply chain

• Software information, i.e., source codes – how it works, what makes it run

• Company information – phone directories, corporate financial data, investment data, budgets, acquisitions, and sales

WHY IS IT EFFECTIVE?

Conferences, conventions, and tradeshows host a wide array of presenters, vendors, and attendees. This provides a permissive environment for traditional and non- traditional collectors to question vendors, develop business/social relationships, access actual or mockups of targeted technology, and interact with subject matter experts.

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

During foreign travel related to attending an event, 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 their hotels.

HOW CAN YOU RECOGNIZE IT?

At conferences, conventions, and 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 from you 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 intelligence officers 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 an individual's personal information that collectors can use to target them later

• Prompting employees to discuss their duties, access, or clearance level

• Attempts to access your electronic devices, i.e., laptop, smartphones, etc

COUNTERMEASURES

• Complete annual counterintelligence 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 at the event

• Prepare responses for questions going into CUI or classified aspects of your product

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

WHAT TO REPORT

Immediately notify your facility security officer 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 for you to act as a foreign sales agent

• Attempts to steer conversations toward your 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 working the booth

• 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

PREPARING FOR FOREIGN VISITORS

PREPARING FOR FOREIGN VISITORS

Foreign visitors are common in today's global economy and are often a welcome opportunity to boost business. However, cleared contractors should be aware that there are potential counterintelligence (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 cleared contractor facilities are one of the most frequently used methods to target and attempt to gain access to controlled unclassified information (CUI) from cleared industry.

RESEARCH AND DEVELOPMENT

It is cheaper for foreign entities to illicitly obtain CUI or classified information and technology than to fund the initial research and development (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 both 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.

TECHNIQUES VISITORS USE TO ELICIT INFORMATION

• ***Peppering:*** Visitors ask a variation of the same question or one visitor asks the same question to multiple U.S. contractor 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 intelligence officers.

• ***Bait and Switch:*** The visitors plan to discuss one business topic, but after arriving, they attempt to discuss the cleared contractor's 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.

PREPARING YOUR FACILITY FOR FOREIGN VISITORS*

• 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 the projects are CUI or classified, are not applicable to the country visit, or include proprietary information.

• If the delegation attempts to make additional contacts with escorts and speakers, ensure they limit discussions to the agreed-upon topics and information.

• Conduct a pre-visit facility walkthrough to ensure visitors cannot hear or see CUI, export-controlled information, or classified information during all areas of their visit.

• 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.

• After the visit, debrief the host and all escorts to uncover if visitors exhibited any strange and/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.

TAKE-AWAY

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 Defense Counterintelligence and Security Agency (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 facility security officer immediately.

EXPLOITATION OF GLOBAL SUPPLY CHAINS

WHAT IS EXPLOITATION OF GLOBAL SUPPLY CHAIN?

Exploitation of the global supply chain refers to foreign intelligence entities' and other adversaries' attempts to compromise a supply chain. This may include the introduction of counterfeit or malicious products into the supply chain with the intent to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communication.

A supply chain is a network of suppliers, manufacturers, developers, warehouses, distribution centers, transportation vehicles, and wholesale or retail outlets. The supply chain may be global. It includes the designers, producers, shippers, and resellers that create, distribute, or influence a product in any way.

Organizations should protect against supply chain threats to the affected system, system component, or information system service. Organizations should employ a standardized process to address supply chain risk as part of a comprehensive, defense-in-depth information security strategy.

Some examples of supply chain exploitation may include, but are not limited to, 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 any disruption to the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an entity
- Intercept, disrupt, or delay shipping
- **Design, Manufacturing, and Assembly:** Personnel that access manufacturing lines or U.S. Government supply chain programs, projects, and systems
- **Technicians:** Personnel that access U.S. Government equipment or systems to conduct routine maintenance or incorporate new components into existing systems/ equipment
- **Software Developers:** Personnel providing code to support both classified and unclassified networks and technology
- **Stock Control Specialists:** Personnel that inventory and control the flow of equipment and material (physical or virtual) in and out of a facility

WHY IS IT EFFECTIVE?

- Successful exploitation of supply chain enables foreign agents, or personnel acting on their behalf, to manipulate Department of Defense (DOD) system components, degrading DOD capabilities and effectiveness during potential conflicts, or to gain access to controlled unclassified information (CUI)
- Counterfeit components will not perform to specification and can include malicious logic intended to degrade or destroy DOD systems and cause events ranging from poor system interoperability, to injury and loss of life, to compromise of national security
- Nonconforming parts are often difficult to identify compared to authentic components
- An actor with insider access could introduce malicious changes or substitutions with a nonconforming part during any phase, increasing difficulty to identify potential malfeasance.

During the design and manufacturing phases, an actor could perform a series of malicious changes, to include: gate-level changes, protocol changes, parameter modifications, wiring modifications, etc.

During the sustainment phase, limited sources for obsolescent components may lead to manufacturers receiving nonconforming parts via gray market suppliers

During the production/testing phase, a part that was intentionally manufactured poorly due to lack of information could cause the user to send the correct specifications back to the bad actor

HOW CAN YOU RECOGNIZE IT?

- Exploitation of the global supply chain can occur at any phase during the process
- During design and manufacturing, personnel should use trusted and controlled distribution, delivery, and warehousing options
- During sustainment, personnel should check for signs of tampering with shipping containers. Personnel also should establish protocols to include independent verification and validation of microelectronics, particularly microelectronics obtained outside of authorized vendors (e.g., obsolete microelectronics)

SIGNS OF A COMPROMISED SUPPLY CHAIN:

- A device that exhibits functionality outside of its original design
- A device or multiple devices from a lot exhibiting a unique error or failure
- 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
- Shipping containers showing signs of tampering

WHAT ARE THE PRIMARY METHODS OF EXPLOITATION?

- Cyber operations
- Personal contact
- Joint ventures
- Tampering

COUNTERMEASURES

To Mitigate Tampering with Components at the Cleared Facility During Assembly/Production:

- Ensure compliance with established security protocols for access to the facility, assembly and production lines, and networks
- Establish and maintain an effective insider threat program
- Train workforce to identify and promptly report suspicious activities

To Mitigate Threat of Counterfeit Components:

- Due Diligence Reporting: Use available resources to look 2-3 levels down the supply chain to vet your downstream suppliers
- 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 their 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

REPORTING

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

Examples of Reportable Activities:

- Devices exhibiting functionality outside the original design
- A device, or multiple devices from a lot, exhibiting a unique error or failure
- Inadvertently or deliberately attempting to break a trusted chain of custody
- Introducing counterfeit components into a USG 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

IMPACT OF LOST TECHNOLOGY

IMPACT OF LOST TECHNOLOGY

In 2012, a U.S. Congress Joint Economic Committee report stated:

"Innovation drives economic growth and job creation. Protection of intellectual property (IP), through patents, trademarks and copyrights, is critical to ensuring that firms pursue innovation. Counterfeiting and piracy erode the returns on innovation and slow economic growth because of the negative impacts on companies, consumers and governments."

Costs of Lost Technology and Intellectual Property:

Loss of technology and IP degrades U.S. national security and economic security.

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 can mitigate U.S. systems' effectiveness or deploy equal capabilities onto the battlefield will cost U.S. and allied warfighter lives

• Adversaries that have equal command, control, communication, and computer, intelligence, reconnaissance, and surveillance (C4ISR) capabilities may gain information superiority over U.S. and allied forces

Economic Impact:

The IP Commission estimated that counterfeit goods, pirated software, and trade secret theft, which includes 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; research and development (R&D) requires investment of resources

• R&D investment includes the risk that the product or process will not be commercially successful

• Foreign competitors can save on the expense and risk involved in R&D by targeting IP at U.S. companies

• IP and technology lost to foreign competitors cost 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 will hurt the company's profitability/fiscal viability

• Eventually, revenue lost to counterfeit goods, pirated software, and lost IP will cost jobs at U.S. companies

WHY TARGET U.S. CLEARED INDUSTRY?

It is cheaper for foreign entities to illicitly obtain controlled unclassified information (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 the U.S. contractors performing R&D a prime target for foreign collection of both classified and unclassified commercial technology.

"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."

IP Commission 2021 Review, Updated Recommendations, March 2021

WHO DO FOREIGN ENTITIES TARGET IN CLEARED INDUSTRY?

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

• **Developers:** Scientists, researchers, engineers, and managers researching and developing leading-edge technologies

• **Technicians:** Personnel who operate, test, maintain, or repair targeted technologies

• **Supply Chain Personnel:** Personnel who source and purchase with a deliverable defense product or technology

• **Information Systems Personnel:** Systems administrators or others with access to cleared facility networks and knowledge of network security protocols

• **Business Development Personnel:** Marketing/sales representatives for domestic and foreign markets

• **Human Resources (HR) Personnel:** HR representatives with access to sensitive information who are public company contacts and initially screen 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:** Scientists/engineers involved with targeted technology publishing in technical journals, participating in professional associations/academia, and patent owners

• **Administrative Staff:** Secretaries, administrative assistants, and executive assistants with access to leadership calendars, contact lists, and company proprietary information

HOW DO FOREIGN ENTITIES TARGET INTELLECTUAL PROPERTY?

• **Exploitation of Business Activity:**

- 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

HOW YOU CAN HELP PROTECT YOUR COMPANY'S INFORMATION

• Adhere to your facility's 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 your facility security officer

"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

REPORTING REQUIREMENTS

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

If you suspect you or your company has been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting counterintelligence (CI) threats and mitigating risks. Reporting allows DCSA to share and address risks with other government and commercial sector partners.

DCSA: https://www.dcsa.mil

DCSA, Counterintelligence: https://www.dcsa.mil/mc/ci

Center of Development: https://www.cdse.edu