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

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 threats and mitigating risks. Reporting allows us to share and address risks together.

> *"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

DCSA
https://www.dcsa.mil

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

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

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

IMPACT OF LOST TECHNOLOGY

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

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