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 counterintelligence (CI) threats and mitigating risks.

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DCSA
https://www.dcsa.mil

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

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

IMPACT OF LOST TECHNOLOGY

Defense Counterintelligence and Security Agency

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 command, control, communication, and computer, intelligence, surveillance, and reconnaissance (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; research and development (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
- Subject Matter Experts
- Administrative Staff

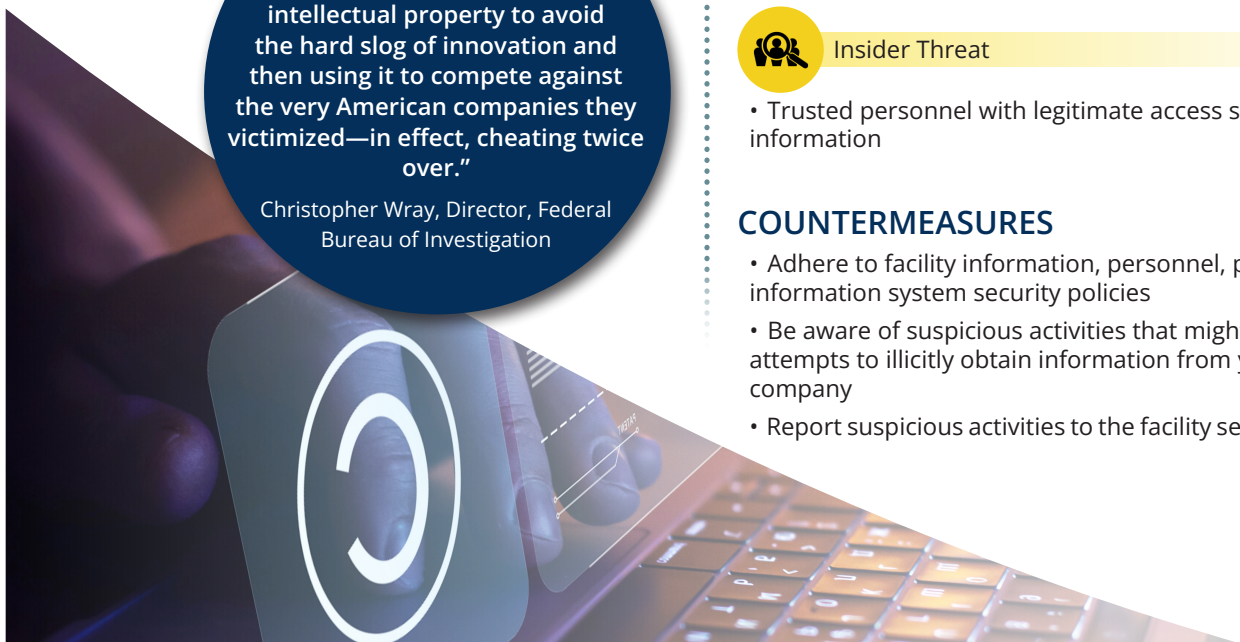
WHY TARGET U.S. CLEARED INDUSTRY?

It is cheaper for foreign entities to illicitly obtain controlled unclassified information (CUI) or classified information and technology than to fund 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.

"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



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

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 facility security officer