U.S. Department of Justice
Federal Bureau of Investigation

Aerospace-Related Economic Espionage

A PERSISTENT THREAT

FBI investigations show economic espionage (EE) and trade secret theft against U.S. Aerospace companies and institutes are on the rise. Over the past five years, foreign actors have targeted U.S. companies, universities, and government research facilities to collect Aerospace technology, expertise, and manufacturing/production capabilities. The FBI leads U.S. Government efforts to mitigate, neutralize, and disrupt the theft of U.S. Aerospace innovations and trade secrets that foreign governments or companies could use to gain an unfair economic advantage and threaten national security.

AEROSPACE-RELATED ECONOMIC ESPIONAGE: A PERSISTENT THREAT

If your company has invested time and resources developing a product or idea – protect it!

AEROSPACE INTELLECTUAL PROPERTY (IP) AND THE THREAT

Aerospace IP includes a company's trade secrets, proprietary information, and research, ranging from avionics to wheels and brakes. Theft of this IP leads to lost revenue, lost employment, damaged reputation, lost investment for research and development (R&D), and disrupted production.

Who Might Steal Your IP?

- Rival or start-up companies.
- Foreign intelligence officers and their sources.
- Non-traditional collectors (researchers, students, businessmen, employees, etc.)
- Disgruntled employees (insider threat).

If your company has a unique product or process that gives you a market edge, you may be targeted. You are your first line of defense in protecting the programs and systems that make your company successful. This is especially true if your company:

- Has a technological edge.
- Has developed a method or procedure to acquire, process, or distribute product(s) at a lower cost than your competition.
- Is negotiating with another company, especially one that is foreign-based.

What is Being Targeted?

Research, test results, production engineering, and sales strategies

- Stealth technology
- Propellant and guidance systems
- Optical/infrared sensors and advanced guidance systems
- Sales and marketing data
- Customer lists

Best Practices to protect Aerospace IP

- Examine your company's information security practices to identify vulnerabilities and mitigate them.
- Clearly identify and safeguard critical information/IP and mark it accordingly (COMPANY PROPRIETARY, PROPIN, CONFIDENTIAL, etc.).
- Do not store proprietary information vital to your company on any device that connects to the Internet.
- Use up-to-date software security tools. Many firewalls stop incoming threats, but do not restrict outbound data. Competitive intelligence hackers try to retrieve data stored on your network.
- Educate employees on spear phishing email tactics. Establish protocols for reporting and quarantining suspicious emails.

You and the FBI: A Partnership to defeat the EE Threat

You are ultimately responsible for protecting your own proprietary information. Congress has continually expanded and strengthened criminal laws for trade secret violations to protect innovation. However, you need to take reasonable steps to protect your IP and products, and document those measures. These laws include:

Title 18 U.S.C., Section 1831 – Economic Espionage is (1) whoever knowingly misappropriate information (e.g. possesses, steal, transmit, download) of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent.

Title 18 U.S.C., Section 1832 – Theft of Trade Secrets is (1) whoever knowingly convert trade secret to the economic benefit anyone other than the owner and (2) knowingly that the owner of the trade secret would be injured. This is commonly referred to as Industrial Espionage.

The International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-1706, which prohibits the violation of regulations issued thereunder, particularly those regulations promulgated by the Department of Treasury imposing trade embargoes and other export restrictions on particular countries, such as Iran and Syria (indictment form and practical skills materials).

Contact your local FBI SPC: SPCs are specially-trained in investigating and identifying Economic Espionage and are available to help you mitigate threats to your organization and trade secrets.

Your local FBI Strategic Partnership Coordinator (SPC) can provide a vulnerability self assessment tool, threat awareness briefings, brochures, and other tools to assist your company. If you believe your company may have been or could become a victim of IP Theft, contact your SPC or the National Intellectual Property Rights Coordination Center.

The FBI will minimize the disruption to your business, and safeguard your privacy and your data during any investigation. Whenever possible, the FBI will seek protective orders to preserve trade secrets and business confidentiality. The Economic Espionage Act of 1996 provides protections for proprietary and trade secret information during trial.

Investigators cannot act if they are not aware of the problem.

You can help the FBI with thwarting Economic Espionage and Theft of Trade Secrets

The FBI welcomes any information you have that could assist with disrupting possible Aerospace EE. Below are questions that will help the FBI understand the threat and assist with ongoing investigations. If you can provide answers, please contact your local FBI Strategic Partnership Coordinator or FBI field office.

- Who are your major foreign competitors in the Aerospace industry? If known, what are their R&D, manufacturing production, and operational capabilities?
- Has your company previously lost talented people to foreign commercial, academic, or government entities involved in the Aerospace Industry? If so, what incentives enticed them to leave (e.g., to work for a competitor, to start up a business, to sell your technology to the highest bidder, foreign government funding, etc.)?
- Which specific programs/offices within your company have liaison relationships/joint efforts with foreign entities? What level of access do the personnel in those offices have?
- Does your company provide counterintelligence (CI) awareness briefs and debriefs to employees who travel abroad for business and personal reasons? What unusual practices have you and your employees observed when traveling abroad and meeting with foreign partners (e.g., surveillance, hotel searching, interrogation, electronics, staff behaving strangely, etc.)?
- Have any cyber intrusions or attacks occurred at your facilities? How would you describe the nature of these incidents (e.g., domain name service (DNS), spear phishing, other)?
- How do you control access to your most critical/emerging technologies? How are your employees trained to protect those technologies? Do non-employees, contractors, or foreign partners have any level of access to these technologies? If so, how are those accesses monitored?

FEDERAL BUREAU OF INVESTIGATION

STRATEGIC PARTNERSHIP COORDINATOR

CONTACT: