Who might steal IP?

- Domestic and foreign commercial rivals.
- Domestic and foreign research facilities.
- Foreign intelligence officers (Spies).
- Disgruntled employees (Insider threat).
  - » Selling IP for profit.
  - » Using IP to create new start up.
- Organized criminals.

Indicators of IP Theft

- Employees/Insiders:
  - » Seeks/Obtains IP not related to their work duties.
  - » Working odd hours to facilitate theft of technology, schematics and/or prototypes.
  - » Unexplained affluence; buying things that he/she cannot afford on their household income.

- IT/Remote Access:
  - » Maliciously or unwittingly downloading and installing Malware.
  - » Blatant theft of data via Universal Serial Bus (USB), electronic mail (email), or Cloud sharing.
  - » Unauthorized access to official laptops/ smartphones (unsecured/lost/stolen).
  - » Transferring data from official laptop while not connected to Virtual Private Network (offsite/telework).

Let us know how we can help you!

Contact your local FBI Office and ask to speak with the SPC so you can safeguard your hard work and keep your people safe.

"America's entrepreneurial spirit and integrity are embodied by the creativity and resourcefulness of our workforce. New inventions, innovations, works of art, and discoveries create jobs and industries and add to our country's heritage. Innovation drives commerce and enables the United States to compete in the global marketplace. Intellectual property rights and the ability to protect those rights encourage American companies to continue the tradition of American innovation by developing products, ideas and merchandise."

ICE Asst Deputy Director Erik Barnett testimony before US Senate Judiciary Committee, 22 June 2011

Contact Information:

Department of Justice
Federal Bureau of Investigation

Counterintelligence Strategic Partnership Programs

The Challenge:

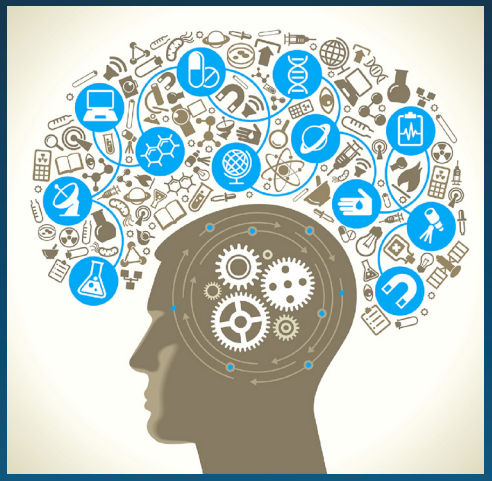
To protect United States corporate and academic Intellectual Property (IP), sensitive information, and technologies from foreign economic espionage activities.

FBI STRATEGIC PARTNERSHIP COORDINATORS - READY TO ASSIST!

Our solution:

Our Counterintelligence Strategic Partnership Program works to determine and safeguard those technologies which, if compromised, could result in significant economic and national security losses. Through our Strategic Partnership Coordinators (SPCs), the FBI initiates and fosters relationships with businesses and academia.

To foster communication and build awareness through partnerships with key public and private entities by educating and enabling our partners to identify what is at risk and how to protect it.



The United States is the world's leader in innovation. Consider the breakthrough research and development taking place on campuses nationwide and within research facilities, often on behalf of the government. Sensitive research, much of which is unclassified, is the key to our nation's global advantage, both economically and militarily.

Strategic Partnership Coordinator (SPC)

Every FBI Field Office has specially-trained Counterintelligence Agents, serving as the primary liaison with their local businesses, cleared contractors and academia. SPC responsibilities include:

- Community outreach to support Counterintelligence and threat mitigation.
- Counterintelligence investigations.
- Facilitate locally-focused and/or Industry specific CI-Threat Working Groups.
- CI Awareness presentations/briefings to local groups, companies, and academia, topics include:
  - » Economic Espionage.
  - » Elicitation Techniques.
  - » Protection of Intellectual Property and Trade Secrets.
  - » Insider Threats.
  - » Risks of Foreign/Competitor visits.
  - » Joint Ventures/Foreign Workforce.
  - » Business Travel/Tradeshows.
  - » Social Networking Risks.
  - » Colleges/Universities Targeted.
  - » Safety Tips for U.S. Students Traveling Abroad.

Your SPC can provide vulnerability self-assessment tools, which will allow you to take an unbiased evaluation of your current threat vulnerabilities. SPCs stand ready to assist your company, university, or research center with the tools to address findings and pro-actively work to mitigate Economic Espionage threats to your Intellectual Property, Research and Development and personnel.

Best practices to protect your IP

Information Technology

- Assess your company's information security vulnerabilities.
- 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/students on spear phishing email tactics. Establish protocols for reporting and quarantining suspicious emails.
- Do not store proprietary/vital information on any device that connects to the Internet. If not entirely possible, review contents and minimize, as practical.
- Clearly identify and safeguard critical information/IP and mark it accordingly. (Both soft/hardcopy).

Employee Education

- Conduct training (at least annually).
- Ensure employees are trained to avoid unintended disclosures.
- Educate employees on techniques used to acquire IP:
  - » Social Media (LinkedIn/Facebook).
  - » Tradeshows and Conferences.
  - » Threats/Blackmail.

Personnel Management

- Ensure Human Resources have policies in-place to specifically enhance information and personnel security.
- Document employee education and other measures to protect IP.

Your SPC is your Advocate for protecting your IP