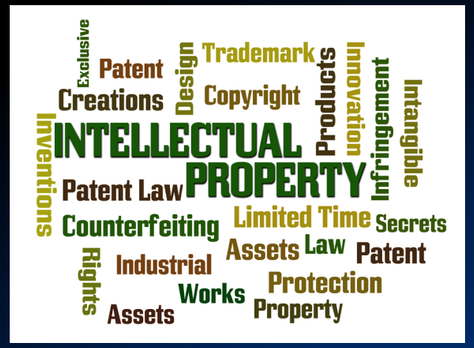
You can help the FBI thwart Economic Espionage and theft of Trade Secrets

The FBI welcomes any information you have that could assist with disrupting possible Oil and Natural Gas (ONG) IP theft. 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.



- What information and technology related to ONG industries are foreign competitors targeting from US businesses, academic institutes, and research entities?
- What are technology gaps of foreign competitors? Are they lacking R&D, manufacturing, production, or operational capability?
- How do US ONG companies collaborate with US academic and government research entities? What ONG research at US companies and academic institutes is supported by federal grants? What ONG research at US academic and government entities is considered proprietary? What is the reasoning process behind this decision?
- How do foreign competitors keep tabs on US research activity and science experts at US companies and academic institutes?
- Which foreign competitors do US companies find most aggressive in pursuing US ONG information and technology? What kind of compromise and penetration activities related to theft of sensitive research and commercial business information have US companies experienced over the past years?

FBI's added value to your company

- Amid changing global energy markets, the FBI can provide expertise delivering recent economic espionage trends against the US ONG industry, raising awareness of current methods adversaries could use to steal trade secrets, and instilling the integrity of your security for your respective shareholders.
- The FBI can identify what global economic and environmental trends may motivate individuals to steal your intellectual property, improving your outward considerations on what items make you a target of, and more vulnerable to, economic espionage.
- The FBI can provide notice of potential security concerns when partnering with suspicious domestic and foreign companies. This ensures business deals meant to increase energy efficiency, diversify supply, and invest in energy production honestly contribute to the future of your business.
- The FBI can provide threat awareness information for consideration during multiple phases of domestic and foreign company partner engagement to assist in ensuring the fidelity of the business relationship.

Contact Information

U. S. Department of Justice
Federal Bureau of Investigation

Oil and Natural Gas Economic Espionage

An Evolving Threat

FBI investigations indicate economic espionage and trade secret theft against US oil and natural gas companies and institutes are on the rise. Over the past two years, foreign actors have targeted and collected against US companies, universities, think tanks, and government research facilities for oil and natural gas information concerning upstream, midstream, and downstream processes. The FBI continues to lead efforts to mitigate, neutralize, and disrupt the theft of US oil and natural gas intellectual property and trade secrets that could be used by foreign governments or foreign companies to gain an unfair economic advantage.

Oil and Natural Gas Intellectual Property and the Threat

Oil and natural gas intellectual property (IP) includes a company's trade secrets, proprietary information, and research. This ranges from drilling equipment to pipeline insulation, which if stolen could result in lost revenue, lost employment, damaged reputation, lost investment for research and development (R&D), and interruption in production.

Who Might Steal Your Intellectual Property?

- Domestic and foreign commercial rivals
- Domestic and foreign start-up companies
- Foreign Intelligence Officers (spies)
- Disgruntled employees (insider threat)
- Organized criminals

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

Best Practices to protect Oil and Natural Gas IP

- Assess your company's information security vulnerabilities and fix or mitigate the risks associated with those vulnerabilities.
- 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 e-mail tactics. Establish protocols for reporting and quarantining suspicious e-mails.
- Ensure your employees are aware of and are trained to avoid unintended disclosures.
- Remind employees to be sensitive to solicitation opportunities while away from their worksites, especially in social settings.
- Remind employees of security policies on a regular basis through active training and seminars.
- Document employee education and all other measures you take to protect your intellectual property.
- Ensure human resource policies that specifically enhance security and company policies are in place. Create clear incentives for adhering to company security policies.

Your local FBI Strategic Partnership Coordinator(s) (SPC) can provide a vulnerability self assessment tool, threat awareness briefing(s), brochures, and other tools to assist your company. If you believe your company may be or is going to be a victim of IP theft, contact your SPC or your local FBI Office. The FBI will minimize the disruption to your business, and safeguard your privacy and your data during its investigation. Whenever possible, the FBI will seek protective orders to preserve trade secrets and business confidentiality.

<u>Investigators cannot act if they are not aware of the problem.</u>

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

You are ultimately responsible for protecting your own IP. Congress has continually expanded and strengthened criminal laws for violations of IP rights to protect innovation; however, you should take reasonable steps to protect your IP and products, and document those measures. These laws include:

Elements of § 1831 Violation

1. Defendant knowingly misappropriated information (e.g., possessed, stole, transmitted, downloaded).
2. Defendant knew or believed this information was proprietary and that he had no claim to it.
3. Information was in fact a trade secret (unless conspiracy or attempt is charged).
4. Defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality or foreign agent.

Elements of § 1832 Violation

1. Defendant knowingly misappropriated information (e.g., possessed, stole, transmitted, downloaded).
2. Defendant knew or believed this information was proprietary and that he had no claim to it.
3. Information was in fact a trade secret (unless conspiracy or attempt is charged).
4. Defendant intended to convert the trade secret to the economic benefit of someone other than owner.
5. Defendant knew or intended that the owner of the trade secret would be injured.
6. Trade secret was related to a product or service used or intended for use in interstate or foreign commerce.

Please contact your local FBI SPC, who is specially-trained in Economic Espionage and is available to assist you with mitigating threats to your organization and intellectual property.

Foreign Competitors Overtly Targeting Oil and Natural Gas Intellectual Property

In 2012, two Chinese nationals were arrested by the FBI for attempting to pay $100,000 to a Project Manager-level employee for "Pipeline Insulation," a trade secret belonging to a well-known US company. The two individuals were seeking the technology to open a plant in China to compete with US companies. They solicited the company's employee via a newspaper ad seeking "technical talent" with 10 or more years experience in "Pipeline Insulation" and a willingness to work in Asia.

The Chinese nationals used low-tech and careless methods of collection. Given the high risk of getting caught, these individuals displayed minimal concern for possible repercussions of their actions. Identified below are espionage indicators noted during the course of this investigation:

- Supplying a company insider with a requirements list through unclassified e-mail.
- Seeking specific types of information at selected companies.
- Targeting a 24-hour operational facility with the highest production of trade secrets, allowing for more opportunities to acquire technology.
- Providing inconsistent information when confronted by plant management for trespassing.
- Asking that trade secrets be provided on a thumb drive.
- Knowingly purchasing documents with proprietary markings with the intention to remove the information.
- Seeking a consultant who can travel to China two to three times a year to support plant developments.