FEDERAL BUREAU OF INVESTIGATION

CHINA: THE RISK TO CORPORATE AMERICA

The annual cost to the U.S. economy of counterfeit goods, pirated software, and theft of trade secrets is between $225 billion and $600 billion.

The Chinese government is the world's principal infringer of intellectual property, and it uses its laws and regulations to put foreign companies at a disadvantage and its own companies at an advantage.

U.S. business interactions with foreign counterparts should be based on the principles of reciprocity, should be grounded in the rule of law, and should seek to uphold our market-based economy and its innovative ecosystem.

The Chinese government, however, does not play by the same rules.

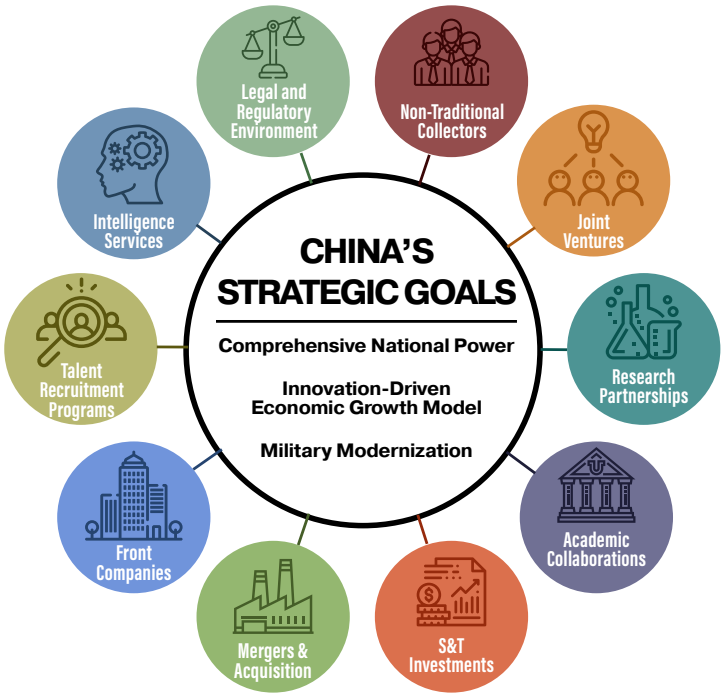
The annual cost to the U.S. economy of counterfeit goods, pirated software, and theft of trade secrets is

$225–$600 BILLION

CHINA'S TECHNOLOGY DEVELOPMENT STRATEGY

China's strategic goals include becoming a comprehensive national power, creating innovation-driven economic growth, and modernizing its military. It aspires to equal or surpass the United States as a global superpower and influence the world with a value system shaped by undemocratic, authoritarian ideals. Using a whole-of-society approach to achieve these goals, China takes advantage of every opportunity—from joint ventures to economic espionage—to develop and maintain a strategic economic edge.

To achieve its strategic goals, China relies on state-directed plans, which provide insight into the kinds of intellectual property and trade secrets the country targets and seeks to acquire from foreign sources. These plans govern foreign acquisition in science and technology, and their scale and influence are impressive.



This document focuses on the activities of the government of the People's Republic of China. References to "China" in this document mean the government of the People's Republic of China.

Made in China 2025 Plan

The Made in China 2025 Plan lists 10 domestic Chinese industries in which China seeks to significantly reduce its reliance on foreign-produced technology and develop 70% of the components for these projects in China:

- Information technology
- Computer numerical control machine tools and robotics
- Aerospace equipment
- Marine engineering equipment and high-tech ships
- Advanced rail transportation equipment
- Energy-efficient and new-energy automobiles
- Electric power equipment
- Agricultural equipment
- New materials
- Biomedicine and high-performance medical instruments

DIFFERENCES IN BUSINESS PRACTICES	
UNITED STATES	**CHINA**
GENERALLY ACCESSIBLE MARKET	HIGHLY RESTRICTIVE MARKET
MARKET ECONOMY	STATE-RUN ECONOMY
DEVELOPMENT BY INNOVATION	DEVELOPMENT BY THEFT, REPLICATION, AND COMMERCIALIZATION
INDEPENDENT JUDICIARY AND SEPARATION OF POWERS	JUDICIARY SUBORDINATE TO THE GOVERNMENT
LAWS PROTECTING INTELLECTUAL PROPERTY	THEFT OF INTELLECTUAL PROPERTY
NO GOVERNMENT-SPONSORED ECONOMIC ESPIONAGE	GOVERNMENT-SPONSORED ECONOMIC ESPIONAGE

CASE EXAMPLE

The director of a Chinese conglomerate and five co-conspirators participated in the theft of inbred corn seeds from fields in the Midwest with the aim of transporting them to China. A U.S. company first notified the FBI of the suspicious activity during a routine liaison outreach meeting. Executives of the U.S. agricultural company estimated the theft would cause them eight years of research and at least $30 million.

The Chinese conglomerate involved in the threat and its seed-developing company is a National Key Dragon Head Enterprises, a designation the Chinese government bestows on private companies in several industrial fields in recognition of the significant role they play in promoting China's modernization. National Key Dragon Head Enterprises enjoy favorable financial support from the Chinese government, including tax exemptions and funding arrangements for commercial loans and lines of credit. Additionally, the Chinese government's Ministry of Science and Technology's 13th Five-Year Plan for Science and Technology Innovation named agriculture seed technology a new, high-priority megaproject.

ACCORDING TO THE CHINESE GOVERNMENT'S STATE COUNCIL, CHINA USES THE FOLLOWING FOUR STEP DEVELOPMENT PROCESS TO GAIN A TECHNOLOGICAL EDGE:	
1 **INTRODUCE**	The Chinese government uses numerous methods—some legitimate but others, such as steal ing technology from foreign competitors, meant to illicitly **introduce** foreign technology and knowledge to China.
2 **UNDERSTAND**	The Chinese government uses its numerous civilian and military institutions and resources to **understand** the materials acquired from foreign sources.
3 **ASSIMILATE**	Those same institutions **assimilate** foreign technology and knowledge into Chinese infrastruc ture—frequently by reverse-engineering it.
4 **RE INNOVATE**	Chinese institutions **re-innovate** foreign technologies, such as military aircraft, high-speed trains, and nuclear reactors, to develop new and state-of-the-art technology. Such advances allow China to achieve generational advances and save time and money on research and development.

FOREIGN TRADECRAFT USED AGAINST BUSINESSES

Corporate Targets of Foreign Adversaries

If your company has a technological edge, expect foreign adversaries to target your technology—including your developmental process and those who have access to your technology. If your company is negotiating with another company or country, foreign adversaries could target your negotiators or negotiation strategy. Some of the information they target might seem insignificant, but by bypassing the research and development phase and stealing your proprietary business information, foreign adversaries can gain a competitive economic advantage.

Foreign adversaries might target your:

- Access protocols
- Acquisition strategies
- Budget estimates or expenditures
- Computer access protocols
- Computer network design
- Confidential documents
- Corporate financial data
- Corporate strategies
- Customer and employee data
- Equipment specifications
- Hiring or firing strategies and plans
- Investment data
- Manufacturing plans
- Marketing strategies
- Proprietary formulas and processes
- Negotiation strategies
- Passwords for your computer, phone, or accounts
- Phone and property data
- Pricing strategies
- Proprietary research, formulas, and processes
- Prototypes or blueprints
- Sales forecasts
- Software, including source codes
- Technical components and plans
- Vendor information and supply chain

CASE EXAMPLE

A U.S. superconductor company sold a Chinese firm wind turbine design and engineering services. Within six years, the Chinese company was the largest wind turbine manufacturer in China and the second largest in the world. It signed contracts to buy $800 million in services from the U.S. company. At the same time, however, the Chinese company recruited a Serbian citizen employed at an Austria-based subsidiary of the U.S. company to download the U.S. company's proprietary control software onto his laptop in exchange for approximately $20,500 and a position within the Chinese company. Once it had acquired the software, the Chinese company no longer needed the U.S. company's support services and immediately severed their business relationship. The Chinese company then produced the software on its own, no longer needing the U.S. company's products. Because of the theft, the U.S. company lost over $1 billion in market capital and laid off more than 70% of its employees.

Foreign adversaries who might target your company's employees, intellectual property, or business information include:

- Foreign commercial rivals and foreign governments
- Foreign academic institutions
- State-owned enterprises—companies that are directed by foreign governments

CASE EXAMPLE

Two individuals and a consulting company were found guilty of economic espionage, theft of trade secrets, and other crimes in a long-running effort to steal a U.S. company's chloride-route titanium dioxide production technology. The individuals sold those secrets for large sums of money to help state-owned Chinese companies develop similar capabilities in China, including a planned 100,000-ton titanium dioxide factory in Chongqing. One of the individuals assembled a team of former company employees to help him send the technology to China. As a result of this theft, the U.S. company reported it lost hundreds of millions of dollars in future revenue.

Tactics China Uses to Target U.S. Businesses and Their Employees

To support its military and commercial research, development, and acquisition, the Chinese government leverages foreign investments, commercial joint ventures, business relationships originating from academic exchanges, and state-sponsored industrial and technical espionage.

Business Techniques

The tactics below all represent legitimate business opportunities for your company. However, foreign adversaries might use any combination of them to strategically target your company.

JOINT VENTURES, including long-term visits, might provide an opportunity for a competing company to obtain restricted information and gain access to a vulnerable collaborative environment. Joint ventures can give foreign companies an opportunity to spot, assess, and befriend employees who might assist—either wittingly or unwittingly—in collecting restricted information during the joint venture or in the future.

Indicators that a joint venture might actually be a threat to a company include:

- A formal connection between the partner company and a state-supported development goal
- Unauthorized access of proprietary information
- Funding provided by a foreign government entity
- Claims by the company with which you plan to partner in foreign patents that it was the sole inventor of products developed in a joint venture
- Obtaining sensitive information without a need to know
- Use of offshore addresses for transshipment points
- Company website under construction for long periods
- Limited information about the company on websites
- Requests from the potential partner company for information on sensitive programs not related to the joint venture

VISITORS entering your facility might pose a security risk to your intellectual property or competitive edge. Some visitors could verbally elicit information, some might brazenly ignore the security restrictions of a tour, and others could use concealed electronic devices to obtain restricted information or access.

ACADEMIC COLLABORATION could open the door to foreign actors who target your employees based on their connections to universities or published scientific research. By participating in collaborative academic opportunities, such as incubators or joint research centers, employees might unknowingly pass intellectual property or confidential information to a foreign adversary. These opportunities to collaborate might also provide an opportunity to spot, assess, and befriend employees who might assist—either wittingly or unwittingly—in passing your research and development to a foreign adversary.

TALENT RECRUITMENT PROGRAMS (also called talent plans) are a vital part of a Chinese government national strategy to enhance Chinese civilian and military programs in key areas critical to China's development. Talent plans integrate foreign technology into China by recruiting experts from businesses and universities across the globe to fill technical jobs that drive innovation and growth in the economy. Various Chinese government talent programs use financial, personal, and professional benefits in exchange for working with universities, businesses, and state-owned enterprises in China.

Talent plans target scientists, engineers, professionals, foreign government employees, and contractors to bring foreign research and technology with them to Chinese universities, businesses, and state-owned enterprises in China. All talent programs constitute a contractual funding source from a foreign government.

Association with talent plans by itself is not illegal; however, potential participants and their current employers should be aware of legal issues that may arise as a result of participation, including economic espionage or violations of export-control laws. A simple download of intellectual property or proprietary information could become criminal activity.

TRADE SHOWS AND CONFERENCES provide a fertile environment for foreign adversaries to assess technology, identify and gain access to company personnel with knowledge of the technology, and illicitly acquire intellectual property. Foreign adversaries target those who want to demonstrate their expertise and are in a position to share their company's information.

FOREIGN TRAVEL can leave U.S. employees vulnerable to targeting through covert searches of luggage and hotel rooms, extensive questioning, manufacture of compromising situations, and confiscation of electronics. Foreign governments do not operate under the same laws or observe the same privacy rights that the U.S. government observes.

ELICITATION of information about your company can come in many forms. A foreign adversary might try to elicit information by using flattery, indicating interest, asking leading questions, claiming a mutual interest, or feigning ignorance.

Insider Threat Risks

Your company is vulnerable to damage from an insider—an employee who has legitimate or illegitimate access to company information and provides that information to a foreign adversary. Insider threats could begin as early as the job application phase, where applicants might be directed by foreign governments to seek employment with access to U.S. trade secrets or proprietary information.

Some of these behaviors might indicate an employee potentially poses an insider threat risk to your company:

- Displays suitability issues, such as alcohol abuse or illegal drug use
- Insists on working in private
- Volunteers to help on classified or sensitive work
- Expresses an interest in covert activity
- Has unexplained or prolonged absences
- Is disgruntled to the point of wanting to retaliate against the company
- Rummages through others' offices or desks
- Misuses computer or information systems
- Unnecessarily photocopies sensitive material
- Attempts a computer network intrusion
- Has criminal contacts or associates
- Employs elicitation techniques
- Displays unexplained affluence
- Fails to report overseas travel, if required
- Works unusual hours
- Takes classified or sensitive material home
- Conceals foreign contacts
- Lacks concern for or violates security protocols
- Attempts to gain access without a need to know
- Shows unusual interest in information outside the scope of his or her job

TO ADDRESS THE POTENTIAL VULNERABILITY INSIDER THREAT RISKS CAN PRESENT, CONSIDER SECURING AND MONITORING TRAFFIC IN YOUR LOCAL AREA NETWORK (LAN). LAN ACCESS IS THE TOP VECTOR FOR INSIDER THREAT EXPLOITATION, FOLLOWED BY PHYSICAL AND REMOTE ACCESS.

CASE EXAMPLE

A senior staff engineer for a major U.S. defense contractor was sentenced to 70 months in prison for exporting sensitive U.S. military technology to China, stealing trade secrets, and lying to federal agents. The engineer stole thousands of electronic files detailing the performance and design of guidance systems for missiles, rockets, target locators, and unmanned aerial vehicles. As part of his plan to position himself for future employment in China, the staff engineer delivered presentations about the stolen technology at several Chinese universities and conferences organized by the Chinese government. On his return flight from China, federal agents found the engineer in possession of a personal computer which contained stolen material related to export-controlled defense items.

Foreign adversaries look for opportunities to exploit your employees' vulnerabilities and motivations to gain access to your intellectual property. In the past, foreign adversaries have targeted the following vulnerabilities when recruiting and exploiting insiders:

- Ideology (such as divided loyalty to a country other than the United States)
- Greed or financial stress
- Ego or self-image
- Coercion or compromise
- Anger, revenge, or disaffection
- The need for adventure or thrills

CASE EXAMPLE

A researcher at a U.S. defense contractor pleaded guilty to charges related to the theft of numerous sensitive military program documents and their transport to China. The researcher let others outside his company know he intended to return to China to work on research projects at Chinese state-run universities using the knowledge and materials he had acquired while employed at the U.S. defense contractor. His research plan indicated China's technology embargo rendered it unable to process high-performance components, such as airplane wings and tailhooks on carrier aircrafts, and the researcher believed his efforts would help China mature its own aircraft engines.

Cyber Techniques

Foreign adversaries might conduct computer intrusions by writing or manipulating computer code to gain access to, or install unwanted software on, your network. To do so, they could employ a variety of techniques.

CLICK-BAITING is when an adversary conceals hyperlinks beneath legitimate clickable content (such as "Like" and "Share" buttons on social networking sites). Once clicked, the links cause a user to unknowingly perform unwanted actions, such as downloading malware or sending the user's ID to a third party.

PHISHING is when an adversary conceals a link or file containing malware in something like an email, text message, or social media message that looks like it is from a legitimate organization or person. If clicked, the link or file compromises the recipient's electronic device and/or associated account.

SOCIAL ENGINEERING is when an adversary tricks a user into divulging confidential or personal information that may be used for fraudulent purposes.

UNPATCHED SOFTWARE EXPLOITATION is when an adversary takes advantage of people or companies that do not update their software regularly to conduct malicious activity, such as computer exploitation or malware installation.

SOCIAL MEDIA EXPLOITATION is when an adversary uses social media networks to exploit a user's personal connections—including his or her profiles, content, and interactions on social media websites—to spot and assess employees for potential recruitment.

CASE EXAMPLE

A federal grand jury indicted five members of China's People's Liberation Army on economic espionage and computer hacking charges. These military members hacked into the networks of six U.S. companies in the nuclear power, metals, and solar products industries—primarily by sending emails to U.S. company employees posing as bank, network, and company officials to obtain passwords, usernames, emails, and other personally identifying information. The Chinese military hackers maintained access to these companies' information for eight years, allowing them to steal trade secrets and other sensitive information for the benefit of Chinese companies, including state-owned enterprises. Stolen sensitive and internal communications also provided the hackers with insight into the U.S. companies' strategies and vulnerabilities.

HOW TO PROTECT YOUR COMPANY

Your organization could consider adopting the measures suggested below to enhance identification and deterrence of potential insider threats. Depending on your company's specific needs, policies, processes, and legal guidelines, you should determine what security measures are necessary to sufficiently protect your company's most important assets.

- Educate and regularly train employees on security policies and protocols.
- Ensure proprietary information is carefully protected.
- Employ appropriate screening processes to hire new employees.
- Implement a continuous evaluation program to persistently screen onboard employees.
- Provide convenient ways for employees to report suspicious behavior, and encourage such reporting.
- Routinely monitor computer networks for suspicious activity.
- Ensure physical security personnel and information technology security personnel have sufficient threat detection software, countermeasure tools, and protective processes in place.
- Provide security personnel with full access to relevant human resources data.
- Conduct exit interviews to identify potential high-risk employees (such as terminated employees and retired employees with insider threat indicators).
- Ensure retired, separated, or dismissed employees turn in all company-issued property.
- Ensure strong nondisclosure agreements and policies restricting the removal of company property.

Develop a Security Strategy

Ensure you have a security strategy to protect your company's information and employees from potential physical and cyber threats. To develop this strategy, identify your company's most important assets and ensure you devote the appropriate resources to their protection. Form teams made up of legal advisors, cyber experts, physical security specialists, human resources specialists, and company supervisors to specifically combat insider threats. Ensure your company's response policies can be easily accessed by employees and that they adequately account for privacy and confidentiality.

Talk to your local FBI field office about any suspicious activities, and request updated threat and awareness materials.

Combating Foreign Adversaries' Tactics to Target Your Company

FOREIGN TRAVEL. To address the potential vulnerability company-related foreign travel can present, when possible, sanitize all electronics to remove intellectual property or personal information before traveling overseas, and check your electronics after you return. Keep your possessions—particularly your identifying documents, phone, and other electronics—with you at all times. If someone gives you things like USB drives, DVDs, or "secure" cell phones before, during, or after a foreign conference, consult your company's security officer before you access them. They may contain malicious software that could compromise or damage your computer systems and steal files from your company.

FOREIGNER VISITS. To address the potential vulnerability foreigner visits to company facilities can present, keep visitor groups together and monitor them at all times during the duration of their visit to company facilities—especially if they have access to areas containing sensitive technology, products, or personal information. When possible, ensure all visitors have proper clearance and background checks before they enter your facilities. Be aware of last-minute additions to visitor lists, as foreign adversaries sometimes add individuals at the last minute in an attempt to steal your information. Prevent unauthorized access to computer systems and ensure visitors do not record your building security access procedures by ensuring visitors do not take videos or photographs or plug portable media devices into company computers.

MALICIOUS CYBER ACTIVITY. To address the potential vulnerability malicious cyber activity can present, monitor logs on these systems to better identify this activity:

- Firewalls
- Proxy
- Web sever
- Anti-virus
- Active directory
- Network Address Translation (NAT)
- Windows event
- Intrusion Detection System (IDS)
- Domain Name Server (DNS)
- Virtual Private Network (VPN)
- Various security appliance logs

If you suspect a cyber intrusion, assess the nature and scope of the incident by isolating the affected systems, target, and origin of the activity. Collect the network logs and records. Implement your company's cyber response plan and report the incident to law enforcement.

When in Doubt, Report the Incident

When in doubt, report a security violation or cyber intrusion to your company's security officer or your local FBI office. *Do not* alert the person under suspicion. Your security officers or law enforcement partners will handle the interaction according to their response policies.

Although your first inclination might be to distance your business from a harmful threat or terminate an employee, there is significant value in reporting a security violation or cyber intrusion to law enforcement. Monitoring and investigating the threat could uncover tradecraft, third party actors, or vulnerabilities to your company.

The FBI places a priority on conducting investigations that cause as little disruption as possible to a victim organization's normal operations. We recognize the need for cooperation and discretion, and, when a problem arises, we will collaborate with your company to determine the best method to address it, focusing on protecting your business's confidentiality, information, and reputation. When necessary, the FBI will seek protective orders to preserve trade secrets and protect business confidentiality.

The FBI is committed to supporting U.S. companies' privacy and competitiveness. As part of this commitment, the FBI can provide security and counterintelligence training or awareness seminars for you and your employees. Private sector companies can apply for membership in FBI-sponsored outreach programs, such as InfraGard and the Domestic Security Alliance Council.

While the FBI is committed to supporting U.S. companies' protection efforts, it cannot do it alone. The FBI relies on U.S. companies to take appropriate precautions to protect themselves from adversaries, both domestic and foreign, who seek to do them harm and steal their proprietary information. The FBI is, and will remain, a willing partner, ready to engage with and support U.S. businesses to protect America's technological and competitive edge from compromise. Whether your company invents, develops, manufactures, tests, or maintains U.S. technology, your partnership with the FBI is critical to protecting your economic interests—and the backbone of our country's vital technologies and national security.

CONTACT US:

For more information, contact your local field office at
https://www.fbi.gov/contact-us/field-offices

WAYS YOU CAN PROTECT YOUR ORGANIZATION There are steps organizations may take to identify and deter potential threats. The FBI offers these for information, but each organization must assess applicability in terms of its own poli cies, processes, and legal guidelines.	NON TRADITIONAL COLLECTORS*	INSIDER THREATS	JOINT VENTURES	FRONT COMPANIES	CYBER
Conduct exit interviews to identify potential high-risk employees (such as terminated employees and retired employees with insider hreat indicators)	●	●		●	
Create a program that regularly screens employees for insider threats	●	●	●	●	
Develop strong risk management and compliance programs			●	●	
Educate and regularly train employees on security policies and protocols	●	●	●	●	●
Employ appropriate screening processes to hire new employees	●	●	●	●	●
Encourage responsible use of social media sites and ensure online profiles have proper security protections in place					●
Ensure the company in question has been vetted through diligent research			●	●	
Ensure physical security personnel and information technology security personnel have the tools they need to share information	●	●	●	●	●
Ensure proprietary information is carefully protected	●	●	●	●	●
Ensure retired, separated, or dismissed employees turn in all company-issued property	●	●			●
Establish Virtual Private Networks (VPNs) for added protection					●
Evaluate the use of nondisclosure agreements and policies restricting the removal of company property	●	●		●	
Install Intrusion Detection Systems (IDSs)					●
Monitor computer networks routinely for suspicious activities	●	●	●		
Negotiate joint venture terms and penalize actions that contradict the agreement			●		
Provide nonthreatening, convenient methods for employees to report suspicious behavior, and encourage such reporting	●	●	●	●	●
Provide security personnel with full access to human resources data	●	●	●	●	
Routinely monitor computer networks for suspicious activities	●	●		●	●
Update software, firewalls, and anti-virus programs					●

**A non-traditional collector is an individual who is not operating on behalf of an intelligence service but who collects information from the United States and other foreign entities to support foreign government–directed objectives.*

For More Information

FBI Private Sector Programs		
ORGANIZATION	**CONTACT**	**ABOUT**
InfraGard	https://www.infragard.org	InfraGard provides a platform for discussion, collaboration, and reporting between the private sector and the FBI. Members can receive FBI cyber intelligence products, such as Private Industry Notifications and FBI Liaison Alert System Messages, and can use the FBI's Malware Investigator tool to share, analyze, and link malware samples.
Domestic Security Alliance Council	https://www.dsac.gov	The DSAC network facilitates a partnership between the private sector and U.S. government agencies focused on discussion, collaboration, and reporting. Members can receive Private Industry Notifications, FBI Liaison Alert System Messages, and other unclassified FBI intelligence products.

Training Materials		
ORGANIZATION	**CONTACT**	**DETAILS**
Federal Bureau of Investigation	http://www.fbi.gov	Numerous publications and videos on the threat from foreign adversaries targeting U.S. businesses.
Center for Development of Security Excellence	http://cdse.edu/catalog/elearning/INT101.html	*Insider Threat Awareness Course (INT101.16)*
Center for Development of Security Excellence	http://www.cdse.edu/toolkits/insider/index.php	*Insider Threat Toolkit*
Emergency Management Institute, Federal Emergency Management Agency	https://emilms.fema.gov/IS0915/index.htm	*Protecting Critical Infrastructure Against Insider Threats (IS-915)*
Software Engineering Institute, Carnegie Mellon University	https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738	*Common Sense Guide to Mitigating Insider Threats, Fifth Edition*

Additional Contacts	
ORGANIZATION	**CONTACT INFORMATION**
FBI Field Offices	https://www.fbi.gov/contact-us/field-offices
FBI Internet Crime Complaint Center	http://www.ic3.gov
National Cyber Investigative Joint Task Force	855.292.3937 | cywatch@fbi.gov
National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security	888.282.0870 | NCCIC@hq.dhs.gov