2008

ANNUAL REPORT TO CONGRESS ON

FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE

This page intentionally left blank.

23 July 2009

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008

This assessment was prepared by the Office of the National Counterintelligence Executive (ONCIX).

NCIX-007-09

This page intentionally left blank.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008

Key Findings

The threat to the United States from foreign economic intelligence collection and industrial espionage has continued unabated since the publication of the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2007*. Economic espionage cases went up slightly and nearly every day brought reports—in the press and in the classified world—of new cyber attacks against US Government and business entities. Additionally, the increasing use of new modes of communication and social networking has provided uncharted opportunities for transferring information and espionage for enterprising foreign intelligence services.

Foreign collectors continued to target a wide variety of unclassified and classified information and technologies in a range of sectors. According to the CI community, which has the most detailed information on foreign collection efforts against dual-use, export-controlled, and military items, the most heavily targeted sectors across all agencies included aeronautics, information systems, lasers and optics, sensors, and marine systems.

Cyber threats are increasingly pervasive, and several key adversaries have drastically expanded their computer network operations for intelligence collection and military use. Moreover, the techniques used and the growing computer globalization made it increasingly difficult to detect and prevent intrusions.

Tracking, analyzing, and countering foreign collection efforts are increasingly complex challenges as the growth of multinational organizations in the global marketplace compounds and obscures the threat to the United States.

This page intentionally left blank.

Scope Note

This assessment is submitted in compliance with the Intelligence Authorization Act for Fiscal Year 1995, Section 809(b), Public Law 103-359, which requires that the President annually provide to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. This report updates the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2007* with data from FY 2008.

As in previous years, this report covers a range of activities—under the rubric of industrial espionage—directed at trade secrets. In this context, trade secrets include financial, business, scientific, technical, economic, or engineering information.

These trade secrets may be tangible or intangible patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes.

They also may be stored or unstored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if the owner (i.e., the person or entity in whom or in which rightful legal or equitable title to, or license in, is reposed) has taken reasonable measures to keep them secret.

In addition, the trade secrets must derive independent economic value, actual or potential, from not being generally known to and not being readily ascertainable through proper means by the public.

Activities to acquire trade secrets include:

- **Economic espionage,** which is the knowing misappropriation of trade secrets with the knowledge or intent that the offense will benefit a foreign government, foreign instrumentality, or foreign agent. Misappropriation includes, but is not limited to, stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to obtain trade secrets without authorization. Section 101(a) of the Economic Espionage Act (EEA) of 1996 criminalizes economic espionage.

- **Industrial espionage**, which is the knowing misappropriation of trade secrets related to or included in a

product that is produced for or placed in interstate or foreign commerce to the economic benefit of anyone other than the owner, with the knowledge or intent that the offense will injure the owner of that trade secret. Misappropriation includes, but is not limited to stealing, copying, altering, destroying, transmitting, sending, receiving, buying, possessing, or conspiring to misappropriate trade secrets without authorization. Industrial espionage is also criminalized under the EEA.

- **Export control violations**, which include:

  Transfer of dual-use equipment and technology: unauthorized acquisition of restricted US dual-use items (having both military and civil applications) by countries or persons that might apply such items in ways that are inimical to US interests. This covers goods and technologies that might be related to the proliferation of weapons of mass destruction and their delivery and those that could bolster the military capability and terrorist activity of certain countries. The Department of Commerce's (DOC) Bureau of Industry and Security (BIS) is responsible for the regulation of exports for national security, foreign policy, and nonproliferation reasons and the enforcement of those regulations. The Federal Bureau of Investigation (FBI) and the Department of Homeland Security's Immigration and Customs Enforcement (ICE) maintain concurrent jurisdiction to enforce violations of these rules. According to the Code of Federal Regulations (28 CFR § 0.85(d)), the FBI is to take charge of the CI aspects of export cases. These organizations coordinate their investigative efforts to ensure that all prosecutorial options are maintained.

  Transfer of defense items: unauthorized export of defense articles, defense services, and related technical data (collectively known as the US Munitions List [ML]). ML items include arms and implements of war. The Department of State's Directorate of Defense Trade Controls administers the International Traffic in Arms Regulations (ITAR), and ICE enforces violations of the Arms Export Control Act and ITAR. The Department of State maintains a policy of denying exports of items on the ML to proscribed countries.

The Office of the National Counterintelligence Executive (ONCIX) compiled this report on the basis of input from US

Government agencies and departments, including the: Air Force Office of Special Investigations (AFOSI), Army Counterintelligence Center (ACIC), Central Intelligence Agency (CIA), Defense Security Service (DSS), DOC/BIS, Department of Energy (DOE), DHS/ICE, Department of State, FBI, National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and the Naval Criminal Investigative Service (NCIS).

This page intentionally left blank.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY 2008

Damaging Theft of US Technologies and Trade Secrets

The threat to the United States from foreign economic intelligence collection and industrial espionage has continued unabated since the publication of the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2007*. Economic espionage cases went up slightly and nearly every day brought reports—in the press and in the classified world—of new cyber attacks against US Government and business entities. Additionally, the increasing use of new modes of communication and social networking provided uncharted opportunities for transferring information and spying on the part of enterprising foreign intelligence services.

According to evidence amassed by the US CI community, a wide variety of foreign entities continued to try to illegally acquire US technology, trade secrets, and proprietary information. With companies encouraging outsourcing of research and development (R&D) and establishing foreign bases of operation, foreign entities had more opportunities to target US information and technologies and mask their collection activities. As a result, it was increasingly difficult to measure fully the extent of their espionage and illegal acquisitions. Nonetheless, the CI community assessed that the cost in FY 2008 remained high, given the number of legal cases, investigations, and technologies targeted.

- The FBI opened 55 new cases and pursued 88 pending cases during the reporting period, slightly more than reported in FY 2007.

- ICE made 158 arrests in FY 2008 and achieved 187 indictments that resulted in 143 convictions for export-related criminal violations, more than any other Federal law enforcement agency. These efforts—similar to the previous year—significantly contributed to preventing sensitive US technologies, as well as weapons, from reaching terrorists, hostile countries, and violent criminal organizations.

- DOC/BIS participated in more than 792 export investigations. This resulted in 40 criminal convictions, $2.7 million in criminal fines, over $800,000 in forfeitures, 56 administrative cases, and $3.6 million in administrative penalties.

Wide Ranging Group of Actors

According to information compiled during the reporting period, businessmen, scientists, engineers, and academics, as well as state security services from a large number of

countries, continued to target US information and technology. The bulk of the collection activity, however, came from a core group of countries.

Enduring Acquisition Methods

While the most frequently reported collection methods remained the same during the past year, requests for information (RFI); exploitation of open-source media; and requests to purchase or share technology were often used. Some reports indicated an increase in the use of multiple methods in single contacts. General techniques included:

RFIs
Collectors used direct and indirect requests for information in their attempts to obtain valuable US data. These types of approaches often included requests for classified, sensitive, or export-controlled information.

Solicitation or Marketing of Services
Foreign companies sought business relationships with US firms that would enable them to gain access to sensitive or classified information, technologies, or projects.

Acquisition of Technology
Collectors continued to exploit direct and indirect acquisition of technology and information via third countries, the use of front companies, and the direct purchase of US firms or technologies in 2008.

Conferences, Conventions, and Trade Shows
These public venues offered opportunities for foreign adversaries to gain access to US information and experts in dual-use and sensitive technologies.

Official Foreign Visitors and Exploitation of Joint Research
Foreign government organizations, including intelligence and security services, also targeted and collected information, frequently through official contacts and visits. Statistics on visits and assignments to DOE facilities indicate that the number of visitors remained relatively stable compared to 2007. The statistics also show that visitors made multiple visits to individual facilities. China and Russia accounted for a considerable portion of foreign visits to DOE facilities during FY 2008 (Figure 1).

Figure 1

Cyber Attack and Exploitation
Cyber threats are increasingly pervasive and are rapidly becoming a priority means of obtaining economic and technical information. Reports of new cyber attacks against US Government and business entities proliferated in FY 2008. Several adversaries expanded their computer network operations, and the use of new venues for intrusions increased. Threats against mobile telephones rose as well. Blackberry and iPhone—essentially general purpose computers—are susceptible to malicious software, according to open-source reporting.

Foreign Targeting of US Travelers Overseas
Foreign collectors also targeted US travelers overseas. Collection methods included everything from eliciting information during seemingly innocuous conversations to eavesdropping on private telephone conversations to downloading information from laptops or other digital storage devices.

Targeted Information and Sectors
Foreign collectors continued to seek a wide range of unclassified and classified information and technologies. Information systems attracted the most attention; aeronautics, lasers and optics, sensors, and marine systems were other top targets.

Looming Concerns

Threat to Emergent Technologies

Emerging, preclassified military technologies or commercial breakthrough technologies are unprotected and are more vulnerable to loss or compromise. Many of these constitute Critical National Assets, defined as systems, processes, technologies, or information that are of broad overriding importance to the survival, safety, or vitality of the United States and that, if stolen, modified, or manipulated by an adversary, would seriously threaten US national or economic security. Often these technologies are difficult to identify in their early phases.

An emergent technologies case involved the University of Tennessee and Atmospheric Glow Technologies. This case was predicated on an alleged conspiracy by Professor J. Reece Roth to transmit export-controlled technical data to a Chinese national. The restricted US Air Force contract involved the development of plasma actuators for a munitions-type unmanned aerial vehicle. A Federal jury in Knoxville convicted Roth of arms export charges in September 2008 and found him guilty of conspiracy to violate the AECA, together with 15 separate illegal exports of military technical information.

DOE identified clean coal energy as a vulnerable technology that might prove central to US economic development strategy in the next decade. This technology was developed as an alternative to converting coal and water into a gas of hydrogen, carbon monoxide, and carbon dioxide that is vented to the atmosphere. To create a clean-burning gas, a DOE-sponsored project has used an Integrated Gasification Combined Cycle to capture harmful carbon and sequester it in the ground. This process remains a leading contender for worldwide adoption. China continues to be a leading competitor in the race for clean coal technology.

Social Networking and Virtual Worlds

The rapid expansion of social networking software and virtual world technology offer new venues for making contacts and transferring information. Virtual world technology—such as Second Life and World of Warcraft—could offer access to information that would be valuable to economic collectors or industrial espionage in the future. The virtual world industry was not as mature as the rest of the World Wide Web, and the tools to protect information were accordingly not as sophisticated.

Appendix A
CI Community Efforts to Protect Technology

The US CI community encompasses a broad set of Federal agencies and departments, each of which works to protect sensitive information and technologies from unlawful foreign acquisition. It includes intelligence collectors, analysts, and law enforcers who meet regularly in a variety of forums to ensure the timely sharing of information and rapid prosecution of key cases. A sample of the support provided by Community members includes:

- **ONCIX** spearheads a number of efforts—including this assessment—that provide impetus to and an organizational hub for the community to combine resources to track CI threats to the nation. The CI community supports the ONCIX Community Acquisition Risk Section (CARS), which evaluates the risk to the IC posed by US commercial entities that conduct business with foreign firms. CARS also provides threat assessments to the Committee on Foreign Investment in the United States (CFIUS) to help ensure that foreign investment does not endanger US strategic interests.

- **AFOSI's** Research and Technology Protection (RTP) program identifies critical Air Force technologies, analyzes threats against those technologies, directs measures to mitigate those threats, and investigates suspicious activities by foreign nationals when warranted. AFOSI also shares RTP-related intelligence with other US Government agencies and cooperatively tracks and analyzes the changing nature of the threat to American technologies.

- **ACIC** supports the Department of Defense (DoD) in characterizing and assessing the efforts of foreign entities—government and private— to unlawfully target or acquire critical US technologies, trade secrets, and proprietary technology information. ACIC produces assessments for technology programs and assesses a foreign country's ability and willingness to protect US technology from unauthorized transfer or disclosure.

- **DIA** assesses foreign intelligence efforts to obtain classified and critical US technologies and examines the means used to collect against US targets and the impact of theft. In addition, DIA supports DoD acquisitions by working with CARS. DIA also helps protect critical DoD technologies through its participation in the IC process to examine foreign ownership, control, and/or influence of US assets and provide input to CFIUS.

- **DOE** facilities and National Laboratories employ a variety of CI countermeasures to protect against the loss of critical nuclear technologies. The DOE Office of Intelligence and Counterintelligence oversees programs to counter the threat from foreign

acquisition, including policy development, field oversight, professional training, awareness training, analysis of CI threats, and investigations and operations support. DOE CI personnel have limited investigative authority to support the FBI in CI investigations and offensive CI operations.

- **DSS** implements the National Industrial Security Program at about 12,000 cleared defense contractor facilities across the United States. On the basis of suspicious incidents reported by contractors, DSS CI traced and analyzed the changing nature of the threat to US technologies. CI specialists teamed with DSS Industrial Security Specialists on nearly 191 security reviews of contractor facilities, using current threat information to assist contractors in developing tailored security countermeasures.

- **FBI's** Counterintelligence Division (CD) is responsible for most of the Bureau's efforts to prosecute and prevent economic espionage in the United States. The division relays the seriousness of foreign threats to US companies, laboratories, and other US entities by providing presentations, publishing tactical and strategic intelligence products, and hosting meetings and working group sessions. Within CD, the Counterespionage Section handles investigations that fall under the purview of the EEA of 1996. This section administratively supports and gives operational assistance to FBI field divisions that undertake these investigations. CD's Domain Section, which began operations in August 2005, oversees efforts to identify and address CI vulnerabilities and threats to critical technologies. The section maintains national security-related liaison initiatives through business and academic alliance programs and provides strategic CI operational leadership through national and regional working groups.

- **NGA's** Office of Counterintelligence works to protect the agency's capabilities, personnel, and facilities. NGA is building the Threat Mitigation Center, which is designed to further integrate and enhance its collaborative efforts in areas such as operational security, industrial security, and information assurance. To achieve synergy between the CI and law enforcement communities, NGA has established a full-time presence at ONCIX CARS. NGA also created a Research Technology Protection Oversight Council to design, develop, implement, and evaluate tactics, techniques, and procedures required to protect new technologies through all stages of the acquisition, research, development, test, and evaluation process.

- **NRO** has worked to improve the identification of espionage threats to its operations, programs, and personnel, as well as increase the awareness of targeting efforts by nontraditional threat countries and groups. In support of its contractor community, the NRO provides tailored briefings of current threats to technology and the targeting methods they employ. In addition, the NRO has streamlined the reporting of foreign contact and foreign travel and disseminates threat information and briefings to security officers and authorized users. The NRO is working closely with the FBI's Domain unit and other mission partners to protect NRO resources and enhance the RTP program. It has also placed a CI representative at CARS to support NRO requirements and the overall CARS mission.

- The **DNI Open Source Center (OSC)** contributes to the CI community's effort against China by monitoring foreign-language publications and Web sites for indications of threats and sharing this information with appropriate agencies, including law enforcement. OSC translates significant open-source materials on CI issues and monitors reporting on economic intelligence and industrial espionage. OSC has taken the initiative in organizing conferences and working groups aimed at countering specific CI challenges and has supported a wide variety of ad hoc requests from offices throughout the IC.

This page intentionally left blank.

Appendix B
Selected Arrests and Convictions for Economic Collection and Industrial Espionage Cases in FY 2008

Country	Technology	Status	Source
China	Space Launch Technical Data	Naturalized US citizen arrested on charges of illegally providing technical assistance and foreign technology acquisition assistance to several Chinese Government entities, September 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
China	Unmanned Aerial Vehicles	US citizen convicted on 15 counts of violating the AECA, September 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
China	Military Aircraft Components	Malaysian citizen pled guilty to conspiring to illegally export military items to China and Iran, August 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
China	Thermal Imaging Cameras	Individual pled guilty to violating the International Emergency Economic Powers Act and the Export Administration Regulations, August 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
China	Amplifiers and Missile Target Acquisition Technology	Florida resident indicted for violating the AECA and International Emergency Economic Powers Act for illegal exports to China, June 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
China	Controlled Amplifiers	US company convicted of knowingly and unlawfully exporting controlled items to China, June 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.

Country	Technology	Status	Source
China	Military Source Code and Trade Secrets	Canadian citizen of Chinese descent convicted of violating the EEA, June 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
Cuba	Specialized Computer Software and Training	US firm charged with trading with the enemy and unauthorized access to a protected computer, July 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
India	Missile Technology	Two US permanent residents convicted of violating the International Emergency Economic Powers Act and the AECA for illegally exporting controlled microprocessors and other electronic components, June and August 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
India	Nuclear Testing Equipment	US firm pled guilty to submitting false export license applications for a proposed shipment of seismic testing equipment with nuclear applications, March 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
Indonesia	Infrared Assault Rifle Scopes	Indonesian national convicted of conspiracy to violate the AECA, July 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
Iran	Engineering Software	Two US citizens, owners of a US firm, convicted of violating the International Emergency Economic Powers Act and The Iranian Transaction Regulations, August 2008.	BIS Export Enforcement, Major Cases List, March 2009.
Iran	Telecommunications Equipment and Technology	US company pled guilty to conspiracy to export to Iran, March 2008.	BIS Export Enforcement, Major Cases List, March 2009.

Country	Technology	Status	Source
Iran	Electronics and IED Components	Eight individuals and companies charged with conspiracy, violations of the International Emergency Economic Powers Act, the US-Iran embargo, and false statements for attempting to ship electronics with dual-use applications, September 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
Iran	Gas Valve Parts	US company convicted of selling parts to Italy for onward shipment to Iran, June 2008.	BIS Export Enforcement, Major Cases List, March 2009.
Iran	Nickel Alloyed Pipes	British corporation pled guilty in US court to one count of violating the International Emergency Economic Powers Act for attempted export without a license, November 2007.	BIS Export Enforcement, Major Cases List, March 2009.
Iran	Fighter Jet Components	US citizen pled guilty to conspiring to illegally export military aviation parts, September 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
Iran	Chemical Purchasing Software	US firm's president indicted for acting as an unregistered agent of the Iranian Government, violating US sanctions against Iran, and lying to Federal agents, July 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
Iran	Cryogenic Pumps	International company headquartered in France pled guilty to conspiracy, illegal export, and attempted illegal export of cryogenic submersible pumps, April 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
Iran	Illegal Export of Three Key Master Software	Naturalized US citizen of Iranian descent, former nuclear plant engineer, pled guilty to transporting stolen property in conjunction with theft of software from a nuclear generating station, July 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.

Country	Technology	Status	Source
Pakistan	Restricted Graphite Products with Nuclear and Missile Applications	US firm sentenced for conspiring to falsify documents and make false statements about a 2003 illegal export to the United Arab Emirates that ultimately ended up in Pakistan, October 2007.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.
Taiwan	Military Laser Aiming Devices and Fighter Pilot Cuing Systems	Taiwan national arraigned on AECA violations after being extradited from Hong Kong, August 2008.	BIS Export Enforcement, Major Cases List, February 2008.
Thailand, UAE	Military Aircraft Components	US firm convicted of making false statements on shipper's export declaration. A company vice president fled and remains a fugitive, July 2008.	DOJ Fact Sheet: Major US Export Enforcement Actions in the Past Two Years, October 28, 2008.