Department of Justice

**STATEMENT OF**

**RANDALL C. COLEMAN**
**ASSISTANT DIRECTOR**
**COUNTERINTELLIGENCE DIVISION**
**FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE**

**COMMITTEE ON THE JUDICIARY**
**SUBCOMMITTEE ON CRIME AND TERRORISM**
**UNITED STATES SENATE**

**AT A HEARING ENTITLED**

**"ECONOMIC ESPIONAGE AND TRADE SECRET THEFT: ARE OUR LAWS ADEQUATE FOR TODAY'S THREATS?"**

**PRESENTED**
**MAY 13, 2014**

**Randall C. Coleman**
**Assistant Director**
**Counterintelligence Division**
**Federal Bureau of Investigation**
**Statement Before the Senate Judiciary Subcommittee on Crime and Terrorism**
**Washington, D.C.**
**May 13, 2014**

Good morning Chairman Whitehouse, Ranking Member Graham, and distinguished members of the subcommittee. I am pleased to be here with you today to discuss the Federal Bureau of Investigation's (FBI) efforts to combat economic espionage and trade secret theft.

*Scope of the Problem*

Theft of trade secrets occurs when someone knowingly steals or misappropriates a trade secret to the economic benefit of anyone other than the owner. Similarly, economic espionage occurs when a trade secret is stolen for the benefit of a foreign government, foreign instrumentality, or foreign agent. Both crimes are covered by the Economic Espionage Act of 1996, Title 18, Sections 1831 and 1832 of the U.S. Code.

U.S.-based businesses, academic institutions, cleared defense contractors, and government agencies are increasingly targeted for economic espionage and theft of trade secrets by foreign entities, often with state sponsorship and backing. The Office of the National Counterintelligence Executive, using estimates from academic literature, has estimated losses from economic espionage to be in the tens or even hundreds of billions of dollars annually to the American economy.

Our foreign adversaries and competitors are determined to acquire, steal, or transfer a broad range of trade secrets in which the United States maintains a definitive innovation advantage. This technological lead gives our nation a competitive advantage in today's globalized, knowledge-based economy. Protecting this competitive advantage is vital to our economic security and our national security. Trade secret theft has hit some of the nation's best-known companies, such as DuPont and Goodyear. To highlight one case in the news earlier this year, a federal jury convicted three defendants in the DuPont case, Walter Liew, Liew's company, USA Performance Technology Incorporated, and Robert J. Maegerle, of 20 charges, including economic espionage and theft of trade secrets. Liew and Maegerle stole trade secrets from DuPont and sold the information to state-owned companies in China.

Fighting economic espionage and theft of trade secrets from U.S.-based companies is a top priority of the FBI's Counterintelligence Division (CD). In 2010, CD created the Economic Espionage Unit, a specialized unit focused solely on prosecuting cases under the Economic Espionage Act. Located within CD's Counterespionage Section, the Economic Espionage Unit works with private sector partners to investigate and prosecute trade secret theft. Within CD, this unit's caseload has continued to

increase every year since its formation. In fact, from FY 2009 to the end of FY 2013, the number of economic espionage and theft of trade secrets cases overseen by the unit increased by more than 60 percent. Economic espionage and theft of trade secrets represent the largest growth area among the traditional espionage cases overseen by CD's Counterespionage Section.

Economic espionage and theft of trade secrets are increasingly linked to the insider threat and the growing threat of cyber-enabled trade secret theft. The employee who poses an insider threat may be stealing information for personal gain or may be serving as a spy to benefit another organization or country. Foreign competitors steal trade secrets by aggressively targeting and recruiting insiders; conducting economic intelligence through bribery, cyber intrusions, theft, and dumpster diving (in search of intellectual property or discarded prototypes); and establishing joint ventures with U.S. companies.

Long gone are the days when a spy needed physical access to a document to steal it, copy it, or photograph it where modern technology now enables global access and transmission instantaneously.

China often is cited as particularly active in the theft of trade secrets. According to a report submitted to Congress by the U.S.-China Economic and Security Review Commission in November 2012, China "depends on industrial espionage, forced technology transfers, and piracy and counterfeiting of foreign technology as part of a system of innovation mercantilism." [1]By obtaining what it needs illegally, China avoids the expense and difficulty of basic research and unique product development, the report concluded. Created by Congress in 2000, the Commission's mandate is to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China.

*Enhanced Strategies for Law Enforcement*

Officials across the U.S. Government are pursuing a comprehensive strategy to counter economic espionage as part of a larger campaign against intellectual property theft. In furtherance of this initiative, the U.S. Department of Justice (DOJ) formed a task force on intellectual property in February 2010. The task force works with the Office of the U.S. Intellectual Property Enforcement Coordinator (IPEC), located in the Executive Office of the President. In February 2013, IPEC issued the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets. The five part strategy calls for focusing diplomatic efforts to protect trade secrets overseas; promoting voluntary best practices by private industry to protect trade secrets; enhancing domestic law enforcement operations; improving domestic legislation; and raising public awareness and stakeholder outreach. The FBI is also a partner at the National Intellectual Property

[1] U.S.-China Economic and Security Review Commission, *2012 Report to Congress*, 112th Cong.,2d session (Washington, DC: Government Printing Office,2012):p.21.

Rights Coordination Center (IPR Center). Together the IPR Center's 21 partner agencies facilitate the exchange of IP theft information among federal government agencies and international partners, plan and coordinate joint domestic and international law enforcement operations, generate and deconflict investigative leads from industry and the public, provide law enforcement training and collaborate closely with industry partners on all forms of IP crime.

The DOJ has also taken steps specifically to address economic espionage. Our partners in DOJ's National Security Division (NSD), for example, are increasingly focused on deterring and disrupting these threats. The FBI works closely with NSD's Counterespionage Section (CES), whose leadership has deep experience and expertise in prosecuting economic espionage and related issues, and whose attorneys are, as the DuPont verdict shows, committed to prosecuting individuals and entities who commit and sponsor economic espionage by any means.

In addition, NSD, together with the Criminal Division, also established the National Security Cyber Specialists Network (NSCS) in 2012. This nationwide network of specially trained prosecutors who focus on cyber threats to the national security, including economic espionage, is actively working with the FBI to build cases against state sponsored cyber threat actors. The NSCS Network has also improved DOJ's outreach to the private sector on cybersecurity issues, including cyber-based economic espionage, both to help prevent intrusions and to improve the government's response when they occur.

*FBI Outreach and Awareness Efforts*

To raise public awareness and conduct stakeholder outreach, the FBI uses the Counterintelligence Strategic Partnership Program (CISPP) to mitigate the risks posed by foreign actors in illicitly acquiring sensitive technologies, advanced scientific research, classified USG information, and trade secrets from private industry and academia. The CISPP network consists of more than 80 special agents experienced in counterintelligence (CI) who are known as Strategic Partnership Coordinators (SPCs). The SPCs counter foreign intelligence threats to academia and private industry by conducting in-person classified and unclassified threat briefings. SPCs provide an early referral mechanism for reports of possible acts of economic espionage, theft of trade secrets, and cyber intrusions. Last fiscal year, SPCs conducted more than 7,500 presentations and briefings about these threats. At the national level, the CISPP manages the Business Alliance and Academic Alliance programs[2], which foster national and local partnerships between the FBI and private industry and academia.

[2] The Business Alliance and Academic Alliance programs develop partnerships with leaders from private industry and academia at the national level through the National Security Business Alliance Council (NSBAC) and the National Security Higher Education Advisory Board (NSHEAB). Both NSBAC and NSHEAB meet quarterly at FBI Headquarters.

SPCs currently maintain more than 15,000 contacts nationwide, consisting of local businesses, academic institutions, and cleared defense contractors. The CI threat briefings and intelligence products provided by SPCs on current trends and indicators help companies detect, deter, and defend against attacks to sensitive proprietary information from foreign adversaries.

This spring, the FBI released a new threat awareness film dramatizing the risks of economic espionage and theft of trade secrets to the American economy. Called *The Company Man: Protecting America's Secrets*, this 37-minute film is based on a trade secrets case recently investigated by the FBI. In the real-life case, a group of conspirators tried to recruit a veteran employee to steal the trade secrets they needed to build a competing plant in China. The film will raise the awareness of audiences about the threat of economic espionage and theft of trade secrets, and help organizations understand the indicators to watch for, so they proactively detect attempts by insiders and foreign agents to illicitly acquire trade secrets and intellectual property. These showings will also encourage viewers to report suspicious activity to the FBI, and help the SPCs build relationships with contacts in local industry and academia. Copies of *The Company Man* DVD have been shipped to the FBI's network of SPCs, who are showing the film and handing out educational materials during in-person screenings. The SPCs answer questions from audience members and are available for short discussions about economic espionage and theft of trade secrets afterwards.

Despite the comprehensive outreach efforts undertaken by the FBI, companies which discover misappropriation of their trade secrets, even misappropriation appearing to rise to the level of criminal trade secret theft, sometimes attempt to address the issue through private negotiations or civil litigation, rather than alert law enforcement. As one example of this problem, during a recent economic espionage investigation at a company, the FBI learned the company had been victimized previously on a separate occasion but pursued a civil action instead of contacting the FBI. The FBI is currently looking into whether this earlier incident involved criminal activity. The FBI is committed to ensuring companies have an established line of communication to report concerns about possible economic espionage or trade secret theft to law enforcement. But the FBI must assure companies the government will work to protect their proprietary information from disclosure during prosecution, so that more companies are willing to come forward and report concerns about possible trade secret theft.

Protecting the nation's economy from this threat is not something the FBI can accomplish on its own. To effectively protect trade secrets, companies need to be proactive—by marking sensitive material as secret or proprietary information, limiting access to protected material, and monitoring who accesses it. Employees should receive regular training, and more frequent notices regarding company policies on protecting trade secrets. Companies should consider implementing non-disclosure agreements with employees to not divulge company proprietary information. If a given piece of information is critical to the long-term success and profitability of a company, the company should limit access to those employees who have a need to know. Further, organizations and companies should evaluate internal operations and policies to

determine if current approaches are tailored to the types of risks and factors associated with trade secret misappropriation committed by corporate and state sponsors. For example, areas for evaluation might include: research and development compartmentalization, information and physical security policies, and human resource policies.

Companies also need to educate their employees about some of the warning signs of insider threat, and regularly explain how to report suspicious behavior. Some of these warning signs include working odd hours without authorization; taking home company proprietary information; and installing personal software, or personal media, on company equipment. Other warning signs include short trips to foreign countries without notification or for unexplained reasons, a sudden influx of wealth, or an employee living beyond his or her means. Companies need to get employees involved in protecting proprietary information and willing to come forward and report concerns about suspicious behavior. In many cases investigated by the FBI, co-workers don't report concerns until after an arrest.

FBI investigators should be contacted as soon as an insider threat is suspected to ensure the passage of time does not hinder any investigation that may be required.

*Increased Penalties for Offenders*

In 2011, the Administration recommended that Congress increase the statutory maximum sentence for economic espionage from 15 to 20 years. In addition, the Administration asked Congress to direct the U.S. Sentencing Commission to consider increasing the guideline range based on aggravated offense conduct in theft of trade secret and economic espionage cases. See Administration's White Paper on Intellectual Property Enforcement Legislative Recommendations, March 2011, at 4-6 (available at http://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf).

In 2012, Congress responded to the growing threat of economic espionage by approving tougher penalties for those convicted of the crime with passage of the Foreign and Economic Espionage Penalty Enhancement Act of 2012. Formerly, an individual responsible for economic espionage faced a maximum fine of $500,000, and organizations faced a maximum fine of $10 million. Congress passed legislation boosting the maximum fine applicable to individuals to $5 million, and organizations responsible for committing economic espionage now face penalties of the greater of up to $10 million or up to three times the value of stolen trade secrets.

Congress also directed the U.S. Sentencing Commission to examine the sentencing guidelines for economic espionage and theft of trade secrets. Following public hearings in 2013, the Commission approved sentencing guideline enhancements where a trade secret is taken out of the country or where a defendant knows the trade secret will benefit a foreign government.

*Challenges*

Often, the greatest challenge in prosecuting economic espionage, as opposed to trade secret theft, is being able to prove that the theft was intended to benefit a foreign government or foreign instrumentality. The beneficiary of the stolen trade secrets may be traced to an overseas entity, but obtaining evidence that proves the entity's relationship with a foreign government can be difficult. The decision to pursue these cases under Section 1832 (theft of trade secrets) instead of Section 1831 (economic espionage) may depend upon the availability of foreign evidence and witnesses, diplomatic concerns, and the presence of classified or sensitive information required to prove the foreign nexus element. Since the law was passed in 1996, there have been 10 economic espionage convictions.

*Conclusion*

Theft of trade secrets and economic espionage is a significant and sustained threat to the nation's economy, and requires constant vigilance. The FBI is working to investigate, and apprehend targets pursuing economic espionage against the United States.

Thank you again for the opportunity to testify. I am now happy to answer any questions you may have.