



C. Frank Figliuzzi  
Assistant Director, Counterintelligence Division  
Federal Bureau of Investigation  
Statement Before the House Committee on Homeland Security,  
Subcommittee on Counterterrorism and Intelligence  
Washington, D.C.  
June 28, 2012

Good morning Chairman Meehan, Ranking Member Higgins, and members of the Subcommittee. Thank you for the opportunity to testify before you today. For the past year and a half, I have had the privilege of leading the FBI's Counterintelligence Division (CD). Our mission is to identify, disrupt, and defeat the efforts of foreign intelligence services operating inside the United States. In the FBI's pending case load for the current fiscal year, economic espionage losses to the American economy total more than \$13 billion. The health of America's companies is vital to our economy, and our economy is a matter of national security. But the FBI, with our partners, is making strides in disrupting economic espionage plots. In just the last four years, the number of arrests the FBI has made associated with economic espionage has doubled; indictments have increased five-fold; and convictions have risen eight-fold. In just the current fiscal year, the FBI has made 10 arrests for economic espionage related charges; federal courts have indicted 21 of our subjects (including indictments of five companies), and convicted nine defendants. In the current fiscal year so far, we have already surpassed the statistics recorded for FY 2011 and expect them to continue to rise. With each year, foreign intelligence services and their collectors become more creative and more sophisticated in their methods to undermine American business and erode the one thing that most provides American business its leading edge; our ability to innovate.

As the FBI's economic espionage caseload is growing, so is the percentage of cases attributed to an insider threat, meaning that, individuals currently (or formerly) trusted as employees and contractors are a growing part of the problem.

According to a February 2012 indictment, several former employees with more than 70 combined years of service to the company were convinced to sell trade secrets to a competitor in the People's Republic of China (PRC). Entities owned by the PRC government sought information on the production of titanium dioxide, a white pigment used to color paper, plastics, and paint. The PRC government tried for years to compete with DuPont Corporation, which holds the largest share of a \$12 billion annual market in titanium dioxide. Five individuals and five companies were commissioned by these PRC state-owned enterprises collaborate in an effort to take DuPont's technology to the PRC and build competing titanium dioxide plants, which would undercut DuPont revenues and business. Thus far, three co-conspirators have been arrested and one additional co-conspirator has pled guilty in federal court. This case is one of the largest economic espionage cases in FBI history.

The insider threat, of course, is not new, but it's becoming more prevalent for a host of reasons, including:

- The pervasiveness of employee financial hardships during economic difficulties;
- The global economic crisis facing foreign nations, making it even more attractive, cost-effective, and worth the risk to steal technology rather than invest in research and development;
- The ease of stealing anything stored electronically, especially when one has legitimate access to it; and
- The increasing exposure to foreign intelligence services presented by the reality of global business, joint ventures, and the growing international footprint of American firms.

To address the evolving insider threat, the FBI has become more proactive to prevent losses of information and technology. CD continues expanding our outreach and liaison alliances to government agencies, the defense industry, academic institutions, and, for the first time, to the general public, because of an increased targeting of unclassified trade secrets across all American industries and sectors.

On May 11, 2012, the FBI launched a media campaign highlighting the insider threat relating to economic espionage. This campaign included print and television interviews, billboards along busy commuter corridors in nine leading research areas nationwide, and public information on the FBI website. Through this campaign, the FBI hopes to reach the public and business communities by explaining how the insider threat affects a company's operations and educating them on how to detect, prevent, and respond to threats to their organizations' proprietary information. Perhaps the most important among these is identifying and taking defensive measures against employees stealing trade secrets.

A recent case underscores the value of the FBI and private companies working together to stop economic espionage and prevent financial losses or breaches of national security. An employee at a Utah company noticed a co-worker download the recipe for manufacturing a proprietary chemical and email it to his personal email account. After this suspicious activity was reported, the company opened its own investigation into the matter and learned that the employee had shared the manufacturing secret with an individual associated with a foreign chemical company. Because of an FBI presentation about economic espionage, company executives called the FBI, and the employee was arrested and charged within 10 days. If businesses, universities, and law enforcement continue to partner together, we can track, apprehend, and prosecute many more individuals suspected of economic espionage.

A second grave threat to our national security is the illegal transfer of U.S. technology. The FBI is seeing an expansion of weapons proliferation cases involving US acquired components. These are components exported from American companies, initially headed to someplace they're allowed to be, but ultimately destined for someplace they should never be. The FBI's Counterproliferation Center (CPC), which identifies and disrupts networks of weapons of mass destruction (WMD) activity, is responsible for pursuing cases of illegal technology transfer, whether the technology is intended for WMDs or other uses. The CPC has tripled its disruptions of illegal transfers of technology since FY 2011. We have made

more than a dozen arrests since the CPC's inception in July 2011, including the arrests of multiple subjects on the Central Intelligence Agency's Top Ten Proliferators List. The CPC has also surpassed statistics recorded for FY 2011 and in FY 2012 (to-date).

One example of this sort of case involved an Iranian proliferation network with associates in Hong Kong, Taiwan, Singapore, and Malaysia, and particularly highlights our partnership with the Department of Commerce's Office of Export Enforcement and Homeland Security Investigations. The network leader targeted dual-use electronic equipment including radio frequency modules. The target obtained this equipment from unwitting U.S. companies and shipped them to intermediary front companies in East Asia before ultimately rerouting the shipments to Iran. Over a dozen of these components have been recovered in caches of improvised explosive devices (IEDs) or recovered as part of the remote detonation systems of the pre- and post-blast IEDs used against American soldiers in Iraq from 2008-2011. Four co-conspirators in Singapore have been arrested and extradition proceedings to the United States to stand trial are ongoing. One US co-conspirator, who worked in research and development at the company manufacturing and shipping these items, pled guilty in federal court this January.

The answer to the threat lies, in part, on the partnerships represented at this hearing. Acting together, we are stronger than when we act alone and are producing results. As we continue our investigative and prosecutorial efforts we make it more painful for individuals and entities to carry out missions related to economic espionage. And as we strengthen and expand public awareness of the threat through our alliances with business and academia, we harden our defenses against those who would do us harm.

Again, thank you for the opportunity to speak with you today. I would be pleased to answer any questions.