STATEMENT FOR THE RECORD
National Counterintelligence Executive
The Honorable Michelle Van Cleave
before the
House Judiciary Subcommittee on Immigration, Border Security & Claims

Hearing on Sources and Methods of Foreign Nationals Engaged in Economic and Military Espionage
September 15, 2005

Mr. Chairman and members of the committee, thank you for the opportunity to testify today on the subject of foreign intelligence threats to America's vital military and other sensitive technologies.

Let me begin by telling you a little about my office, the National Counterintelligence Executive (NCIX), which was created in the wake of a series of debilitating spy scandals that rocked our nation over the past decade and a half. You will no doubt remember Aldrich Ames, a former CIA counterintelligence (CI) officer, who was arrested in 1994. He spied for the Russians for nearly a decade, during which period some 30 operations against the Soviets were compromised, and at least 10 Russians and East Europeans were executed as a result of his espionage. Indeed, as the Senate Intelligence Committee reported, Ames was responsible for the loss of virtually all of CIA's human intelligence assets targeted at the Soviet Union at the height of the Cold War.

At the time, it was believed that Ames was the most damaging spy in U.S. history, but, in fact, there were others also spying at that time who would vie for that title. FBI Agent Robert Hanssen, arrested in 2001, spent at least 21 years serving the same master as Ames. He compromised sensitive programs and intelligence capabilities that cost the U.S. Government more than $22 billion. Also hard at work for another country, Cuba, was the lesser known, but potentially no less damaging spy, DIA analyst Ana Montes. She spent 17 years betraying our country.

The losses that these and scores of other spies inflicted resulted in grave damage and danger during peacetime; they could have had catastrophic consequences had we found ourselves at war. Now we are at war with terrorists and facing continuing threats from other adversaries, and the potential consequences of intelligence failure are far more immediate, putting in jeopardy deployed forces, ongoing operations, and the lives of troops abroad as well as Americans at home. Indeed, each of the major challenges confronting the nation's security today—defeating global terrorism, countering weapons of mass destruction, ensuring the security of the homeland, transforming defense capabilities, fostering cooperation with other global powers, and promoting global economic growth—has an embedded counterintelligence imperative. We must protect against those who engage in a range of intelligence activities directed against U.S. interests and objectives at home and abroad.

To counter continuing espionage and other foreign intelligence threats against America's national security secrets, and to deal with these new challenges, the United States requires a national, systematic perspective and coherent policies, including a strategic counterintelligence response. It is for exactly these reasons that the Congress created the position of the NCIX. The CI Enhancement Act of 2002, which established my office, directs that the NCIX head national counterintelligence for the U.S. government, subject to the direction and control of the Director of National Intelligence. As NCIX, I chair the National CI Policy Board, which is the principal mechanism for developing policies and procedures for the approval of the President to govern the conduct of CI activities. I also lead a 64-person Office of the National Counterintelligence Executive (ONCIX), which is now within the office of the DNI.

ONCIX has the core mission of providing strategic direction to the nation's counterintelligence efforts overall. Specifically my office is responsible for:

- Developing the National CI strategy, an unprecedented effort in the annals of U.S. counterintelligence.
- Providing annual assessments of the foreign intelligence capabilities of our adversaries and the threat they pose to the United States.
- Overseeing and coordinating strategic analyses on critical CI issues, as the threat, technology, and our interests and vulnerabilities continue to evolve.
- Drafting assessments to gauge and help remediate the damage inflicted by the spies we have caught, such as Ames, Hanssen and Montes.
- Developing and setting priorities for CI collection requirements across the Community.
- Developing policies and standards for training and educating CI professionals in the challenging art and tradecraft of CI.
- Fostering heightened public awareness of basic CI threats to our nation.
- Providing budget guidance for the CI Community to ensure that the nation's resources are focused on the key CI tasks outlined in the National CI Strategy.

Nearly 140 nations and some 35 known and suspected terrorist organizations currently target the United States for intelligence collection through human espionage and by other means. Their purposes are many: to steal our national security secrets to support their war aims or terrorist objectives, or to undercut us in foreign policy or commerce, or to exploit what they learn of our intelligence capabilities to hide their actions or mislead us. If left unanswered, their success could come at dear cost, putting in jeopardy U.S. operations, military and intelligence personnel, and Americans at home.

Effective counterintelligence is a strategic imperative to protect American lives and operations and to support the advance of freedom.

In March of this year, the President approved the nation's first National CI Strategy, which I would like to submit for the record. Its purpose is to direct and unify U.S. counterintelligence activities to achieve strategic objectives in support of the nation's security. The Strategy speaks directly to the critical issues that are before this Committee today: protecting critical U.S. technologies, trade secrets, and sensitive financial or proprietary economic information from foreign collectors.

The foreign theft of sensitive dual-use and military technologies has eroded the U.S. military advantage by making dangerous technology available to our adversaries. In addition, it has degraded the U.S. Intelligence Community's ability to provide information to policymakers, and it has undercut the competitiveness of U.S. industry by allowing foreign firms to acquire, at little or no cost, technology that U.S. firms spent hundreds of millions of dollars developing.

Stopping the illicit foreign acquisition of sensitive U.S. technologies must be addressed through a combination of national security tools: export control laws, diplomatic measures, industrial security arrangements, limits on foreign investment in strategic U.S. industries, and counterintelligence.

It is the job of U.S. counterintelligence to identify the foreign intelligence hand orchestrating efforts to acquire sensitive U.S. technologies. The primary focus of CI is to defeat the efforts of foreign intelligence services to acquire U.S. national security secrets. It is also our job to support larger national policy efforts to stem the outflow of sensitive technologies. My office was created, in part, to contribute this essential CI policy piece to our nation's national security and homeland security objectives.

Sensitive U.S. technologies—those that both underpin the U.S. economy and contribute to U.S. military prowess—remain prime targets for foreign acquisition, both lawful and illegal. To this end, foreign companies, scientists, academics, and others see the acquisition of U.S. technology as key to advancing their economic and military interests.

A World of Increased Foreign Access to Sensitive U.S. Technology and Trade Secrets

The globalization of the U.S. economy and the explosive growth in technology, especially information technology (IT), have been double-edged swords. Some of the very factors that have significantly contributed to U.S. economic growth and technological progress have at the same time facilitated foreign entities' technology acquisition efforts against us. For example:

- Our general culture of openness has provided foreign entities easy access to sophisticated technologies. Each year, for example, we allow tens of thousands of official foreign visitors into U.S. Government-related facilities such as military bases, test centers, and research laboratories. Some of these visitors are dedicated to acquiring U.S. technology and know-how not otherwise available.

- American colleges and universities, centers for high-tech development, employ large numbers of foreign born faculty and train large numbers of foreign students, many of whom will return to their home countries. For example, an increasing number and share (approaching 30 percent) of science and engineering faculty employed at U.S. universities and colleges are foreign born, according to National Science Foundation statistics. Moreover, the most recent data available indicate that about 40 percent of the PhDs awarded by U.S. universities in technical sciences and engineering—roughly 8,000 per year—now go to foreign students. The vast majority of these students are legitimately studying and advancing academic pursuits. But some are not.

- Breathtaking advances in IT have vastly simplified the illegal retrieval, storage, and transportation of massive amounts of information, including trade secrets and proprietary data. Compact storage devices the size of a finger and cell phones with digital photographic capability are some of the latest weapons in technology transfer as are the tools of cyberspace.

- Sophisticated information systems that create, store, process, and transmit sensitive information have become increasingly vulnerable to cyber exploitation. Many nations have formal programs for gathering our networked information, and foreign competitors are developing the capability to exploit those vulnerabilities.

- Globalization has mixed foreign and U.S. companies in ways that have made it difficult to protect the technologies these firms develop or acquire, particularly when that technology is required for operations overseas. In 2004 alone, according to the Department of Commerce, foreign investment in the United States amounted to more than $100 billion. A couple of the notable foreign acquisitions of U.S. high-tech companies in the past few years include the purchase of fiber optic network provider Global Crossing by Singapore Technologies and the more recent takeover of IBM’s personal computer business by China’s computer giant Lenovo.

The Major Threats

Given the access that foreigners have to U.S. technology and the importance of that technology to their economic and military development, it should be no surprise that individuals from many countries are involved in the creative acquisition of U.S. technology including theft. In FY2004 alone, the CI Community tracked efforts by foreign businessmen, scientists, academics, students, and government entities from almost 100 countries to acquire sensitive U.S. technologies.

In order to discuss in detail the specific countries involved in this technology transfer, we would need to go into closed session, but a couple of points about the collectors are notable. First, while the number of countries seems large, in fact, most of the activity was conducted by individuals from a very few locations. The top 10 collectors, for example, probably accounted for 60 percent or so of the suspicious foreign collection efforts against U.S. cleared defense contractors last year, according to reporting from the Defense Security Service. The countries in that top-10 list are a diverse group. They include some of our closest allies as well as some of our adversaries. Among them are countries where per capita income levels are high as well as those at the other end of the scale. Two countries that always rank near the top of the list and that are frequently cited in the press are, of course, China and Russia.

It is difficult to determine how much of the theft of U.S. sensitive technology is being directed by foreign governments and how much is simply being carried out by private businessmen, academics, or scientists for purely commercial or scientific reasons. Importantly, in many cases we do not know how much of a nexus there is between the private and public sectors that are targeting our technologies. Anecdotal evidence and incomplete statistical information indicate that much trade secret and technology theft takes place without direct intervention by foreign governments, though most foreign governments that are involved do not discourage such theft and themselves often benefit from the transfers. It is clear, however, that the major threat countries continue to employ state organs—including their intelligence services—as well as commercial enterprises, particularly when seeking the most sensitive and difficult to acquire technologies. In addition, we note that a number of countries have begun to establish institutions at home and in the United States to take full advantage of technology acquired by private citizens working or studying here.

The Methods of Operation

We face significant intelligence gaps in understanding how foreign nations collect against U.S. technology. But there are a number of things the CI Community can say with confidence about the perennially serious problem of state-sponsored industrial espionage. For example, we know that a number of the major foreign intelligence agencies have:

- Dedicated programs whose primary task is technology acquisition. These programs often involve the use of front companies, which operate surreptitiously.

- “Laundry lists” of targeted technologies and specific strategies for acquisition. Where an entire system cannot be acquired, foreign intelligence services may attempt to steal component parts.

- Arrangements to share technology that has been both legally and illegally acquired with other countries’ intelligence and security services, even when the sharing of that technology is itself illegal.

Overall, the techniques used to acquire sensitive U.S. technologies are far broader than those traditionally associated with espionage. In the case of China, for example, its national-level intelligence services employ a full range of collection methodologies, from the targeting of well-placed foreign government officials, senior scientists, and businessmen to the exploitation of academic activities, student populations, and private businesses. The Chinese intelligence efforts take advantage of our open economic system to advance China's technical modernization, reduce the U.S. military advantage, and undermine our economic competitiveness. Let me highlight for you some of the relatively new methods that China and other state and non-state collectors sometimes use to gain access to our technology. As might be expected, the techniques that are easiest to use, least expensive, and lowest risk are the ones first and most often employed.

For example, **in a majority of cases, foreign collectors simply ask—via e-mail, phone call, FAX, letter, or in person—for the information or technology.** When a foreign request for U.S. technology is either refused by a U.S. company or the U.S. firm asks the foreign firm to apply for an export license, the foreign company often simply breaks off communication and looks for another possible U.S. seller. With search costs extremely low, the foreign firm can afford to continue looking until it locates a U.S. company that either does not understand the export licensing requirements or is willing to ignore them in order to make the sale.

Another common technique employed by foreign entities is to exploit visits to U.S. businesses, military bases, national laboratories, and private defense suppliers. Recognizing the mutual benefits of an unhindered exchange of information, the United States opens its military bases, national laboratories and private defense suppliers to foreign visitors. Even foreign students and academics visiting U.S. universities where high-tech experiments are underway can present problems. The CI Community receives incident reports about foreign experts wandering into restricted areas, peppering U.S. researchers or scientists with questions well outside the range of issues they are supposed to discuss, and taking photographs of sensitive equipment that the foreign experts are not supposed to see.

The losses that result from such visits can be significant. Such foreign visitors are often among their nations' leading experts and, as such, may be much more effective at extracting sensitive information than would be traditional foreign intelligence officers. Specialists know their countries' or companies' specific technological gaps and can focus their collection efforts directly on the critical missing information. Finally, such experts are also in a position to recognize and exploit information that may be inadvertently exposed during visits.

And the technology losses to long-term foreign visitors can be even more significant than those to foreign experts making shorter visits. For one thing, overseas specialists who stay on site for extended periods of time become familiar with, and learn to circumvent, the security procedures meant to limit their access to sensitive technologies. This is particularly true of cyber security procedures. A long-term presence may allow visitors time to acquire passwords and to learn where on hard drives sensitive information is stored. Whereas short-term visitors are viewed as strangers on sensitive sites, long-term visitors become part of the landscape. Their activities naturally receive less notice, which enables them to wander into sensitive areas without attracting undue attention.

Increasingly the CI Community is most concerned about cyber tools being used in efforts to extract sensitive information. The insider threat—an individual with access to a U.S. firm's computer system but actually working for a foreign entity—is, of course, of most concern. But the Community is also worried about other cyber exploitation techniques, including probing, scanning, phishing, spamming, virus dissemination and the use of sophisticated hacking tools, many of which are available online. Cyber exploitation is inherently difficult to detect as cyber intruders from one country typically cover their tracks by routing their attacks through the compromised computers of others. At the same time, the losses can be significant and finding the cyber bandit can be virtually impossible.

U.S. businessmen traveling abroad provide another valuable source of information for foreign countries. Foreign governments and businesses continue to acquire sensitive U.S. proprietary information from all types of electronic storage devices, including laptop computers, personal digital assistants (PDAs), and cell phones carried by U.S. businessmen traveling abroad. A recent U.S. private sector study indicated that two-thirds of PDAs are used to carry client details and corporate information but without adequate protection. Foreign businesses and security services gain access to such information by using clandestine entry to hotels and business establishments or by electronically downloading information during routine security inspections at airports or other ports of entry. In addition, technology weaknesses in some PDAs make it easy for foreign entities to extract information without directly accessing the storage devices.

Foreign students, scientists, and other experts who come to the United States to work or attend conferences also can serve as a funnel for sensitive U.S. technologies. China, in particular, seems to be benefiting from the access its experts have here. The Chinese press explicitly recognizes the role of the overseas Chinese community in increasing China's technological prowess. Moreover, Beijing has established a number of outreach organizations in China and it maintains close relations with a number of U.S.-based advocacy groups that facilitate its interaction with experts here and probably aid in efforts to acquire U.S. technology.

One indirect method used to acquire U.S. technology is for foreign firms to offer their services or technology—particularly IT-related support—to U.S. firms that have access to sensitive items. Such deals, at a minimum, have provided foreign visitors access to facilities where trade secrets or proprietary information are stored. In their most dangerous forms, however, these deals can result in foreign companies subverting U.S. firms' supply chains by selling tainted products. These subversions could give foreign companies long-term, remote access to significant proprietary information and trade secrets. Well-executed supply chain subversions are almost impossible to detect, even years after implantation.

In some cases, foreign entities seeking to acquire sensitive U.S. technologies find that the easiest route to acquisition is to **either purchase outright or form a joint venture with a U.S. firm that has access to that technology.** Even joint venture negotiations where no agreement is reached can yield proprietary information valuable to foreign entities. The negotiation process often includes plant tours and inspections of manufacturing processes, and the U.S. firms may provide proprietary information on customers and marketing plans in an effort to secure the deal.

Increasingly, foreign entities need not even come to the United States to acquire sensitive technology but, instead, can work within their own borders. There, U.S. firms have difficulty securing their secrets and have few legal protections once proprietary information has been lost. Globalization is forcing U.S. companies toward a more diversified business model that includes foreign outsourcing and external partnerships. These arrangements, while making U.S. firms more competitive by providing a source of inexpensive inputs, at the same time make sensitive U.S. technologies more vulnerable. For example, a recent security survey by a major U.S. accounting firm showed that sensitive blueprints, formulas, and computer codes are being transferred abroad to enable foreign firms to supply specially tailored inputs to high-tech products that are manufactured in the United States.

Conducting due diligence on foreign partners is difficult, but the problem becomes geometrically more complicated when the foreign partners themselves outsource to other firms. According to the same security survey just cited, fewer than one-third of U.S. companies that are involved in outsourcing conduct regular assessments of their IT providers to monitor compliance with information security policies; "they simply rely on trust." These trends not only leave U.S. firms more exposed to a direct outflow of technology but also make it difficult to guarantee that the foreign-provided inputs—particularly IT hardware and software—are free from Trojan horses or back doors that could be used later to extract sensitive technology.

The Technologies Targeted

What kinds of technologies are targeted? Virtually all kinds of U.S. trade secrets—military and civilian—are targeted. The CI Community pays closest attention to technologies with direct military application and to those on the Defense Department's Militarily Critical Technologies List (MCTL), many of which are dual-use, with both military and commercial applications. All of the technologies on the MCTL are targeted every year. **Information systems**—the foundation of almost all modern civilian and military production processes—continue to top the list of targeted technologies. There has also been significant foreign interest in **sensors**, which provide the eyes and ears of many military systems; **aeronautics**, because of the demonstrated advantage of airpower in recent international conflicts; **electronics**, which are either contained or used in the production of virtually every weapons system in the U.S. arsenal; and **armaments and energetic materials**, the technologies required to develop and produce conventional munitions and weapons systems of superior operational capability.

As difficult as it is for us to track foreign efforts to acquire military and dual-use technologies—where defense contractors are required to report suspicious targeting incidents—it is far more challenging for the CI Community to monitor foreign targeting of purely commercial technologies. The FBI has outreach programs that are geared to encouraging U.S. firms to report suspicious targeting incidents but, even so, such reporting is uneven at best. U.S. firms have sometimes been reluctant to raise alarms about possible technology theft out of concern for the potential impact on investor and consumer confidence and stock prices. Nevertheless, recent legal cases alleging technology theft provide examples of the items targeted, which include: semiconductor production processes, computer microprocessors, high-speed digital cameras, software, proprietary information, and chemical formulas.

The Rough Road Ahead

We should expect no decline in foreign demand for sensitive U.S. technologies over the next few years. The United States remains the source of much of the world’s most advanced technology, and, in many industries, foreign entities depend on that innovation to improve their competitiveness. At the same time, the task of slowing the illicit outflow of technology will only become more difficult. Globalization, while benefiting the United States economically, is making it challenging to isolate trade secrets from foreign managers and employees. Increasingly U.S. firms are conducting research and development in centers located outside U.S. borders, where physical security will be difficult to maintain and legal protection of technology, trade secrets, and innovation is weak or nonexistent. At the same time, however, U.S. businesses prefer to operate in an environment where their trade secrets are protected, which may gradually pressure foreign governments to strengthen legal safeguards.

It is one thing to list the range of foreign technology acquisition activities to you; it is quite another to describe what we need to do about them.

In my view, successful policy must be consistent, and thoughtfully apply the full range of public policy instruments to strategic effect. For its part, U.S. counterintelligence has to be more effective than the foreign intelligence services—meaning more pro-active in identifying, assessing and degrading foreign intelligence operations against us.

My office has underway an aggressive program to identify, align and coordinate the many CI community efforts to slow this illicit outflow of U.S. technology. We are grouping these activities as the centerpiece of our implementation planning for the National CI Strategy and the recommendations of the Silberman-Robb Commission. Major efforts include, for example, the work of the FBI-led national CI working group on technology protection and a number of cyber threat and technology vulnerability response initiatives.

Mr. Chairman, your Committee has jurisdiction over our nation's single greatest resource in countering foreign intelligence threats, the Federal Bureau of Investigation. The most significant change of late, and it is significant indeed, is the President's June decision to create a new National Security Bureau within the FBI. The integration of counterterrorism, counterintelligence, and intelligence programs in the new NSB should give a major boost to our nation's CI capability, and to achieving the objectives of the National Counterintelligence Strategy.