Michelle Van Cleave
Senior Fellow, Homeland Security Policy Institute
George Washington University
Statement before the

House Committee on Science, Space, and Technology
Subcommittee on Oversight
May 16, 2013

Espionage Threats at Federal Laboratories:
Balancing Scientific Cooperation while Protecting Critical Information

Mr. Chairman,

Thank you for the opportunity to appear today to discuss the foreign intelligence threats to America's science and technology enterprise. Having served as head of U.S. counterintelligence under President George W. Bush, I can tell you that foreign intelligence services are far more active against us … and far more successful … than most Americans would ever imagine possible.

The most intense and dangerous foreign espionage efforts are directed against what we might call traditional targets, e.g., the secrets of our weapons laboratories, or the operational specifications of our intelligence satellites, or our military plans and capabilities, or the sensitive decision making apparatus of our government. But it doesn't stop there.

In fact, foreign collectors are interested in virtually all aspects of U.S. economic activity and technology, and their numbers are growing. According to the National Science Foundation, America invests some $15 trillion annually in R&D, more than all of the G-8 combined. So it is little wonder that we are the world's candy store for other powers looking to gain advantage on the cheap: by stealing it.

While some of this illicit activity may be opportunistic, the larger threats are purposeful and strategically directed and coordinated. As I will explain, this is hardly a new phenomenon but it is growing in significance and scope. Some of the very factors that historically have contributed to U.S. economic growth and technological progress have at the same time facilitated foreign entities' technology acquisition efforts against us. Human collection is integrated with cyber operations in ways that magnify the reach of both. And it is far from clear that our intelligence insights are deep enough, or our policies effective enough, to address the strategic implications of these threats.

This is a reality that is sharply at odds with the free and open values that underpin the world of science and research and the expansion of knowledge. As the National Research Council wrote in its 2007 study on science and security,

> The task of achieving the appropriate balance between the need for rapid, open communication among scholars and the safeguarding of information that could be used to do us harm is a challenging one, and it is one that requires the continual and sustained attention of the scientific community. The… nation can and must strike this balance so that our extraordinary creativity and productivity can continue to flourish and propel us into a prosperous future.[1]

The question is, is the current balance "appropriate"? And how would we know if it was not?

Russia

Let me begin by telling you a success story out of the Cold War. At their very first meeting, newly elected French President Francois Mitterrand brought President Reagan a very special gift. Mitterrand confided that French intelligence had a source, deep inside the KGB, who was providing unparalleled information about Soviet technology acquisition from the West. Thanks to this source, codenamed "Farewell," western intelligence gained invaluable insights into Soviet intelligence tasking and collection operations directed against our R&D and technology base.

"Farewell" revealed that the Soviet Union had built an intricate network of state organizations to carry out focused and wide-ranging technology acquisition activities to support its military buildup. In addition to the KGB and the GRU (military intelligence), these included the State Committee for Science and Technology, the Ministry of Foreign Trade, and the State Committee for Foreign Economic Relations. The Soviet Academy of Sciences also played a role in obtaining documents and facilitating contacts.

Among other things, "Farewell" was able to provide the central Soviet "shopping list" for U.S. technologies. We learned that Soviet weapons production planning included express requirements for the acquisition of Western technologies or parts, as an integral feature in their weapons development work. So in effect, the U.S. was subsidizing the Soviet economy and in particular its military buildup.

The insights provided by "Farewell" – whose real name was Vladimir Vetrov -- played a significant role in our winning the Cold War. The Soviet economy was stretched thin and they depended on access to western technologies to support their military aims. With their "shopping list" in hand, the U.S was able to join with NATO and other allies to control the export and sale of dual use technologies, as well as to undercut KGB "Line X" collection efforts through other creative means. For his part, after landing in jail for other reasons, Vetrov later was convicted of espionage by the Soviet authorities and executed.

---

[1] National Research Council of the National Academies of Sciences Committee on a New Government-University Partnership for Science and Security, Committee on Science, Technology, and Law Policy and Global Affairs, *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities (*Washington DC: The National Academies Press) 2007, p5.

Why dwell on this story from the Cold War Past? Well, (as that former U.S. President might have begun), because today, everything old is new again … but with a better public relations campaign. Mikhail Fradkov, the current head of the SVR (the successor to the KGB) helpfully explains, "Intelligence aims at supporting the process of modernization of our country and creating the optimal conditions for the development of its science and technology."

Translation: "Farewell" may be out of business, but the old KGB Line X (technology acquisition) practices are not.

In fact, the numbers of Russian intelligence officers and operations in the United States today are easily at Cold War levels. The time and effort and treasure Russia devotes to these activities provide some indication of the rate of return Moscow gets from that investment. And with long practice, they know what they are doing – with the added advantage that, in the aftermath of the Cold War and with so many other demands on U.S. national security, we are perhaps not watching as closely as we once did.

China

Still, when it comes to stealing western technology, China is giving Russia a run for its money. China's intelligence services employ a full range of collection methodologies, from the recruitment of well-placed foreign government officials, senior scientists, and businessmen to the exploitation of academic activities, students populations, and private businesses. These Chinese intelligence efforts take advantage of our open economic system to advance China's technical modernization, reduce the US military advantage, and undermine our economic competitiveness.

According to the Defense Department's 2013 report on PRC military activities,

> The Chinese utilize a large, well-organized network to facilitate collection of sensitive information and export-controlled technology from U.S. defense sources. Many of the organizations composing China's military-industrial complex have both military and civilian research and development functions. This network of government-affiliated companies and research institutes often enables the PLA to access sensitive and dual-use technologies or knowledgeable experts under the guise of civilian research and development. The enterprises and institutes accomplish this through technology conferences and symposia, legitimate contracts and joint commercial ventures, partnerships with foreign firms, and joint development of specific technologies. In the case of key national security technologies, controlled equipment, and other materials not readily obtainable through commercial means or academia, China has utilized its

intelligence services and employed other illicit approaches that involve violations of U.S. laws and export controls. [2]

So in a manner reminiscent of the old Soviet practices, China has an extensive government apparatus and highly coordinated tasking and collection activities targeting U.S. technologies. Consider also that these same tasking and collection operations can be and are put to use in acquiring intellectual property and other proprietary information of commercial value. And business is booming, thanks in part to growing employment of Chinese nationals in U.S. facilities as well as the off-shoring of U.S. production and R&D to facilities in China.

During the Cold War, we understood Soviet objectives to be adversarial to our own; and there was a western alliance of free nations working closely together to protect and preserve our collective security and advance our common prosperity. The United States had a carefully developed strategy concerning the Soviet Union, articulated in such seminal Presidential directives as Truman's NSC-68 and Reagan's NSDD-75. This strategic guidance also ordered our response to identifying and disrupting illicit technology acquisition activities by the USSR.

No such clarity of purpose exists with respect to U.S. interactions with China. In my view, some of the deficiencies in U.S. policy toward Chinese economic espionage and other illicit activities targeting U.S. R&D derive in no small measure from the absence of a larger strategic framework guiding U.S./Chinese relations.

Disturbing Trends

By far the vast majority of foreign acquisition of U.S. technology is open and lawful, as are the transactions of individuals and businesses involved in international commerce, as well as the free exchange of ideas in scientific and academic forums. But let me turn to the cases that fall outside the bounds of what is open and lawful – a category that is growing in scope and import.

The last year I was in office, we tracked efforts by foreign businessmen, scientists, academics, students and government entities from almost 100 countries to acquire sensitive U.S. technologies protected by export control laws or other means. Of those, the top 10 countries accounted for about 60% of the suspicious foreign collection efforts against cleared defense contractors. The two countries that always rank at the top of the list are of course Russia and China, which have particularized interests especially in dual use technologies with military application. But the top ten also included certain of our allies, who sometimes exploit their easy access to push the envelope into areas where they have not been invited.

In recent years, U.S. counterintelligence has observed more interaction among collectors from different countries and different regions. As the Pentagon's Defense Security

[2] Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*, pp 11-12.

Service (DSS) explained last year, "Whether working with each other, working through each other, buying from each other, or attempting to throw suspicion on each other, these convoluted pathways make it more difficult to ascribe collection attempts to a particular country, region, or collector affiliation."[3]

In other words, it's a crowded field. And the prognosis is not good. According to the same DSS report, the total number of incident reports from industry in 2012 went up 75% over the past two years, continuing a relentless upward trend at roughly the same pace for the past decade.

In fact, each year the reports out of U.S. counterintelligence and security reflect figures that are worse than the year before. Losses are growing. Numbers of collectors are growing. Vulnerabilities are growing. And the erosion of U.S. security and economic strength is also growing. It reminds me a little of Senator Dirksen's famous remark, "A billion here and a billion there and soon you're talking about real money."

Mr. Chairman, we're talking about real money. For fiscal year 2012, the FBI estimated that losses to the United States from economic espionage totaled more than $13 billion. Other analyses suggest that figure may significantly understate the true costs:

- ***Underreporting***. As difficult as it is 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 US firms to report suspicious targeting incidents but, even so, such reporting is uneven at best. US 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.

- ***Dynamic costs.*** The National Science Foundation calculates that the U.S. invests about 2.8% of our GDP annually in R&D … or some $436 billion in 2012. R&D is the engine for new ideas and concepts and products and wealth. How much of that national treasure is targeted by foreign collectors to fuel their business and industry (and government programs)? What are the dynamic costs to the U.S. economy (in lost competitiveness, jobs, market share, etc.) as a result?

When one adds in cyber collection, the estimates of real losses skyrocket. The Director of the National Security Agency, General Keith Alexander, has called cyber espionage "the greatest transfer of wealth in history." I would say that cyber exfiltration is of a piece with a global rats nest of technology and intellectual property theft.

[3] Defense Security Service, *Targeting U.S. Technologies 2012: A Trend Analysis of Reporting From Defense Industries*, p6

Why are things getting worse?

Globalization has been wonderful for business and commerce and the free flow of ideas and information, bringing greater opportunities for trade, investment, growth, cultural and personal exchange and the expansion of knowledge.[4] It has also been wonderful for spies.

Our general culture of openness has provided foreign entities easy access to sophisticated technologies. Each year, recognizing the mutual benefits of an unhindered exchange of information, we allow tens of thousands of official foreign visitors into US Government-related facilities such as military bases, test centers, and research laboratories. For example, NSF statistics show that 60% of postdocs employed at Federally Funded R&D Centers are foreign born nationals on temporary work visas. And each year, the counterintelligence 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 security procedures meant to limit their access to sensitive technologies. The insights thus gained may enable them to circumvent those security practices. 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.

---

[4] According to the U.S. Travel Association, there were over 62 million international arrivals into the United States in 2011. Between 2004 and 2011 (the most recent Commerce Department statistics) the number of Russian visitors to the U.S. more than doubled, with most of the increase in business and professional travel. The number of Chinese visitors over the same period more than quadrupled.
http://tinet.ita.doc.gov/outreachpages/download_data_table/2011_Russia_Market_Profile.pdf
By 2016, DoC forecasts that Russian visitors will be up another third, while the number of Chinese visitors will nearly triple again.
http://www.ustravel.org/sites/default/files/page/2009/09/US_Travel_Answer_Sheet_Jan2013.pdf

Similarly, 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. The vast majority of these are legitimately studying and advancing academic pursuits. But some are not.

Globalization has also 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. Foreign direct investment in the United States currently stands at $3.1 trillion – the highest on record, according to the Commerce Department. The Committee on Foreign Investment in the United States (CFIUS), which advises the President on the national security implications of proposed foreign investments and acquisitions, has seen its workload grow75% in the last few years.[5] Having had responsibility for providing intelligence assessments to the CFIUS when I served as the National Counterintelligence Executive (NCIX), I am concerned that our insights into the nexus of foreign business, industry and government programs fall short of satisfying those requirements.

And then there is the Internet. The information revolution is enabling once unimagined processing, transmission and storage of data, empowering the individual and opening our world to extraordinary new horizons. It has also altered the face and prospects for espionage, in scope and scale. The "Wikileaks" postings are but the tip of the iceberg of the challenge facing the government in protecting U.S. national security secrets, or industry protecting its proprietary information, or individuals protecting their privacy.

As this Committee is keenly aware, 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 and employing the capability to exploit those vulnerabilities, interjecting a whole new dimension of national security threat and risk. The jury is out whether proposed legislative or other remedies will help better protect our nation's information systems or deter or defeat cyber exploitation or attack.

What are they interested in?

Our national laboratories are the guardians of some of our nation's most closely held and vital secrets. As such, they are targets of extreme interest by foreign powers seeking to acquire those secrets. The first time our nuclear weapons secrets were stolen, it led to a 50-year Cold War with the Soviet Union. In the late 1990s, the Cox Commission revealed that China acquired through espionage design information on all nuclear weapons currently in the U.S. inventory…and we still don't know how they did it.

Other sensitive areas of federally funded R&D are clearly of great interest to our adversaries as well – as are the propriety secrets and intellectual property of American business and industry. The latest NCIX report on economic espionage assesses that the

[5] Committee on Foreign Investment in the United States, *Annual Report to Congress 2012*, p3.

greatest foreign interest is in information technologies, military technologies, and civilian/dual use technologies in sectors likely to experience fast growth such as clean energy, health care, and pharmaceuticals.

In 2012, DSS found that the top four most targeted technology categories were unchanged from the year before: information systems, lasers, optics and sensors; aeronautics systems; and electronics. Armaments and energetic materials came in fifth, with a growing interest in technologies for processing and manufacturing, directed energy, and space systems.

I would invite the Committee's attention to the prominent position of aeronautics and space systems on the list of foreign interest. The launch of Sputnik some 56 years ago, which led to the creation of this Committee, was a technology challenge and a national security shock that profoundly changed the way the U.S. government approached science and technology. From that point forward, it did not require much of a visionary to understand that space would be critical to national defense – or that its enabling technologies would be coveted by adversaries and competitors.

The Chinese, in particular, are keenly interested in space technology, in which America is still the world's unquestioned leader. Just ask 30-year spy Dongfan Chung (Orange County, Calif.) or Shu Quan-Sheng (Newport News, Va.) or Lian Yang (Seattle), now serving time for passing inter alia space-shuttle communication technologies, space-launch cryogenic fuels data and satellite semiconductor devices, respectively. And that's just the tip of the iceberg.

Collection activities

There are significant intelligence gaps in understanding how foreign nations collect against U.S. technology. However, we do 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.

- Programs that provide funding for students and businessmen who assist in collecting intelligence information.

In other words, foreign targeting of the U.S. science and technology base is driven by purposeful collection, tasking and exploitation by foreign nations who employ the full reach of their intelligence capabilities to that end. Moreover, the techniques used to acquire sensitive US technologies go beyond those traditionally associated with espionage. The rich network of human interaction, business and commerce that is innocent and open and above-board provides excellent cover for the sliver of activity that is none of that. Let me review some of these techniques.

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

U.S. businessmen, scientists and academics traveling abroad provide another valuable source of information for foreign countries. Foreign governments and businesses also acquire sensitive US proprietary information from all types of electronic storage devices, including laptop computers, personal digital assistants (PDAs) and cell phones carried by US businessmen traveling abroad. 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.

In some cases, foreign entities seeking to acquire sensitive US technologies find that the easiest route to acquisition is to either purchase outright or form a joint venture with a US 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 US firms may provide proprietary information on customers and marketing plans in an effort to secure the deal.

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. Marketing pitches can elicit useful information. Sales can get foreign firms (and foreign collectors) inside the U.S. concern … which may be all they need to walk off with sensitive proprietary information … or to facilitate remote access to computer systems for future exploitation. 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.

Foreign collectors may exploit joint research undertakings or visits to U.S. businesses, military bases, national laboratories, and private defense suppliers, to extract protected information. In particular, DSS noted that "[p]lacing academics at U.S. research institutions under the guise of legitimate research offers access to developing U.S. technologies and cutting-edge research" in such areas as information systems, lasers, aeronautics and underwater robots.

Foreign students, scientists, and other experts who come to the United States to work or attend conferences also serve as a funnel for sensitive U.S. technologies. For example, a student may seek a postdoctoral position or other job with a cleared contractor, thereby gaining access to sensitive or classified technologies to support parallel R&D efforts in their home countries. China, in particular, seems to be benefiting from the access its experts have here. The Chinese press explicitly recognizes the role of the overseas community in increasing China's technological prowess. Moreover, Beijing has established a number of outreach organizations in China to help maintain contact with its overseas community and facilitate technology transfer, groups such as the Overseas Chinese Affairs Office, the Chinese Overseas Exchange Association, the State Administration of Foreign Expert Affairs, etc. China also supports a number of US-based advocacy groups that facilitate its interaction with its experts here, including the Association of Chinese Scientists and Engineers, the China Association for Science and Technology, and the Chinese Institute of Engineers.

According to the FBI, ***foreign intelligence targeting of U.S. colleges and universities in on the increase.*** For example, in 2009 Michigan State University was approached by a Dubai based concern offering to fund their extension campus in Dubai – which (as reported in the press) later turned out to be a front for Iran; MSU said "no thanks.". Attempts by countries in East Asia, including China, to obtain classified or proprietary information by "***academic solicitation***," such as requests to review academic papers or study with professors, jumped eightfold in 2010 from a year earlier (as reported by DSS); such approaches from the Middle East doubled.

The late Sergei Tretyakov, the highest ranking Russian intelligence officer ever to defect while stationed in the United States, managed Russian intelligence operations out of New York from 1995 through 2000. In his words, "We often targeted academics because their job was to share knowledge and information by teaching it to others, and this made them less guarded than, say, UN diplomats."[6] This included satisfying collection taskings from Moscow such as "a study of genetically engineered food being done at New York University."[7]

Increasingly, foreign entities need not even come to the United States to acquire sensitive technology but, instead, can work within their own borders. There, US firms

[6] Former Deputy Rezident Sergei Tretyakov quoted in Pete Earley, *Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War* (New York: G.P. Putnam's Sons, 2007) 196.
[7] *Ibid* at 194.

have difficulty securing their secrets and have few legal protections once proprietary information has been lost. Globalization is forcing US companies toward a more diversified business model that includes foreign outsourcing and external partnerships. These arrangements, while making US firms more competitive by providing a source of inexpensive inputs, at the same time make sensitive US technologies more vulnerable.

Conducting due diligence on foreign partners is difficult, but the problem becomes far more complicated when the foreign partners themselves increasingly outsource to other firms. 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.

It is difficult to determine how much of the theft of U.S. sensitive technology and intellectual property is being directed by foreign governments, rather than self-initiated by companies or academics or unscrupulous entrepreneurs. But the more we learn about illicit technology collection, the more we see patterns that reveal the hand of foreign government involvement. So for example the 2012 DSS report attributed a large number of cases to government entities which would likely have been designated "unknown affiliation" in the past.

Even where there may not be central government direction and control, most foreign governments that are involved do not discourage such theft and themselves benefit from the transfers. For example, Chinese universities and research institutes in particular have associations with their nation's militaries, which means that students and academics are likely to contribute to military R&D following completion of their studies or research fellowships. Think of it as part of the study abroad experience to bring back something useful when you come home.

U.S. National Strategy and Policy

The history of technology security policy debates is long and contentious, and marked by a lack of clear authority or uniform practices, despite volumes of outside commissions, recommendations for improvement, and internal substantive reviews. Yet technology protection regimes are only as strong as their weakest link. Inconsistent practices among government agencies and especially the divide between national security departments and agencies on the one hand, and at-risk agencies not within the national security community on the other, are a persistent problem.

In my view, government policy is most effective when we coordinate the full range of public policy instruments so they are applied to strategic effect. Stopping the illicit foreign acquisition of sensitive U.S. technologies requires a combination of national security tools, including export control laws, diplomatic measures, industrial security arrangements, limits on foreign investment in strategic U.S. industries, and counterintelligence. Each of these merits scrutiny, to ask whether they are properly

conceived, resourced and implemented in light of the growing threats to the U.S. science and technology base and the fundamental values they are meant to protect.

It is also worth exploring what gaps may exist in national policy and strategy. For example, there are no post-employment restrictions on federal employees from going to work for foreign firms, even firms with close ties to the military. Accordingly, Huawei has been hiring key U.S. talent… including (according to press reports last year) the former head of the cybersecurity division of the Homeland Security Department. Former U.S. government employees are barred by law from disclosing classified information, to be sure; but they walk off the job with specialized knowledge and understanding informed by their intimate familiarity with sensitive programs and operations. When I stop to think what we could learn if the roles were reversed – if senior Chinese government employees were to be hired away by US companies secretly employed by the USG to penetrate Chinese markets or critical infrastructure – I find myself wondering if we shouldn't take a closer look at this particular revolving door.

Among other things, Congress has a vital role to play in advancing awareness of foreign intelligence activities directed against our R&D base, including such activities as today's hearing. Awareness begins with educating the S&T community and the public – as well as our national leadership -- about the threat. In that regard, the National Research Council Report, which I cited earlier, was occasioned in part at the urging of this Committee. The time may be ripe for the National Academies to commission a fresh look. Certainly in the six years since their last report was issued, foreign targeting and exfiltration of sensitive U.S. R&D and technology have risen sharply. Perhaps there is more that the S&T community could be doing to help.

The larger solutions fall to national policy leadership and the security disciplines. How do we weigh the risks of foreign visitors and researchers at our federal R&D establishments against the benefits of scientific exchange and the value of collaboration? Are existing vetting and security procedures well designed and enforced? How do we protect information of value in all its forms, from paper to digital to conversations in person or at a distance? Do security and awareness training enable personnel to understand why they are being asked to take safeguards, or are they just handed a set of rules?

And most significantly, do we have a national capability to counter foreign intelligence operations that threaten our economic prosperity and national security? The scorecard of America's counterintelligence enterprise falls short of the growing strategic foreign intelligence threats directed against us, to include the extraordinary creativity of our S&T enterprise. We need better insights into what foreign intelligence services are doing and how they are doing it, and a genuine national strategic counterintelligence program, so that we might stand a better chance of stopping them.

Conclusion

This is likely not the first time the members of this Committee will have heard that we are facing growing foreign intelligence threats targeting U.S. science and technology; indeed, I am sensitive to the fact that such warnings may sound like a broken record which, in time, loses its appeal. But I have endeavored today to provide some of the reasons why I believe you should take that warning to heart.

In closing, I want to say that it is a special honor for me to be here, having served as minority counsel to this Committee in 1989. Accordingly, I am familiar with the unique jurisdictional responsibilities of HSS&T, and I commend the Oversight subcommittee for taking on the difficult questions raised by today's hearing. I hope it will give you a starting point for more detailed inquiry into the security practices of our federal laboratories and related national policies affecting America's science and technology enterprise. Thank you and I look forward to your questions.