U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight

HEARING CHARTER

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

Thursday, May 16, 2013
2:00 p.m. – 4:00 p.m.
2318 Rayburn House Office Building

Purpose

On May 16, 2013, the Subcommittee on Oversight will hold a hearing titled *Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation while Protecting Critical Information*. The goal is to gain an understanding of how federally-owned-or-operated laboratories balance scientific openness and international cooperation with the need to protect sensitive information from espionage. This hearing will focus on identifying potential deficiencies, best practices, and to ensure sensible federal policies.

Witnesses

- Dr. Charles M. Vest, President, National Academy of Engineering;
- Dr. Larry Wortzel, Commissioner, U.S.-China Economic and Security Review Commission;
- Hon. Michelle Van Cleave, Senior Fellow, Homeland Security Policy Institute, George Washington University;
- Mr. David G. Major, Founder and President, The Centre for Counterintelligence and Security Studies.

Background

The United States has long been the world leader in higher education, science and technology and a magnet for foreign-born scholars, scientists and engineers. Unfortunately, various actors have sought to exploit our openness to steal American ingenuity and innovation. Such thefts can enable nations to save themselves billions in research and development costs and make technological advances they would be unable to make on their own to gain a competitive industrial advantage or modernize their military and other national capabilities.

Historically, restrictions focused mostly on technologies with obvious military applications such as nuclear material, cryptography and biological weapons. The goal of American counterespionage was to prevent a potential adversary from gaining such technological

advantage, and during the Cold War, it was generally clear what nations should be guarded against. However, the emergence of transnational terrorist actors and the means of communicating information, including technological innovation, via the Internet, has given rise to a far greater, more diverse and global espionage threat.

In the United States, there has long been support for a policy of not restricting publication of federally supported research results, except where classified for national security reasons. This position was best expressed in 1985 by President Ronald Reagan in National Security Decision Directive 189 (NSDD-189), which remains the government policy regarding controls on federally-funded research results. The directive asserts that "to the maximum extent possible, the products of fundamental research remain unrestricted."[1]

Fundamental research is defined within NSDD-189 as:

> "…basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."[2]

NSDD-189 acknowledges that there are risks associated with the open exchange of ideas within the scientific and academic communities, but it asserts that the benefits to security and other key national objectives outweigh the potential dangers.[3] Nonetheless, the emergence of significant threats to national security has at times caused the pendulum to swing toward increased security and tighter controls at the cost of scientific openness and international collaboration.

Benefits of International Scientific Cooperation

Science is a worldwide endeavor. In 2008, American Association for the Advancement of Science (AAAS) Chief Executive Officer Alan I. Leshner testified before this Committee that, "Science is by definition global in scope and application - it knows no borders, is not constrained by geography, and no one country has a monopoly on it."[4]

In March 2011, Bo Cooper, former General Counsel to the then-Immigration and Naturalization Service (INS), testified before the House Judiciary Committee that, "Throughout our history, our country has operated on the principle that the more brain power we can attract from around the

[1] White House, Executive Office of the President, "National Policy on the Transfer of Scientific, Technical, and Engineering Information," National Security Decision Directive-189, 1985, available at: http://www.aau.edu/WorkArea/showcontent.aspx?id=1560; hereinafter NSDD 189.
[2] Ibid.
[3] Ibid.
[4] Written Testimony of Alan I. Leshner, House Committee on Science and Technology, Subcommittee on Research and Science, "The Role of Non-Governmental Organizations and Universities in International Science and Technology Cooperation," 110th Cong., 2d sess., 2008.

world, the more creativity, invention, and growth we can achieve here at home."[5] A Harvard Business School study found that the number of inventions, as measured by patents, increased when H-1B visa caps were higher due to "the direct contributions of immigrant inventors."[6] Though the numbers have declined during the current economic downturn, immigrants with advanced degrees still comprise a considerable percentage of U.S. workers in science and engineering occupations. At the doctoral degree level, about half of U.S. workers in computer and mathematical sciences and in engineering are foreign-born.[7]

Aside from sparking innovation and entrepreneurship, foreign scholars make significant contributions to the American economy. The Association of International Educators estimates that international students and their dependents contributed approximately $21.8 billion to the American economy during the 2011-2012 academic year. This figure is based on an analysis of tuition, enrollment figures, living expenses and other associated costs.[8]

International scientific cooperation and openness to international students also serves longstanding and important U.S. foreign policy goals by fostering communication and cooperation among nations to promote greater global peace, prosperity and stability.

Intelligence Threats to Science and Technology Community

According to the Office of the National Counterintelligence Executive, foreign economic collection and industrial espionage is a significant and growing threat. Russia and China are the most aggressive and persistent perpetrators.[9] While China's intrusions of U.S. computer networks has increased significantly in recent years, China's espionage continues to operate in the physical world as well. Chinese scientists and engineers permeate U.S. academic and industrial research sectors. While most are honest, hard-working individuals, here in the U.S. for legitimate reasons, a quick review of recent economic espionage and trade-secret theft cases involving Chinese scientists and engineers show a more systemic campaign to gain American know-how:

- In November 2012, Shanshan Du and Yu Qin were convicted for conspiring to steal hybrid technology from General Motors on behalf of a Chinese competitor.

---

[5] Written Testimony of Bo Cooper, House Committee on the Judiciary, Subcommittee on Immigration Policy and Enforcement, "H1B Visas: Designing a Program to Meet the Needs of the U.S. Economy and U.S. Workers," 112th Cong., 1st sess., 2011.

[6] William R. Kerr and William F. Lincoln, "The Supply Side of Innovation: H-1B Visa Reforms and Us Ethnic Invention," (Working Paper 09-005, Harvard Business School, 2008), available at: http://www.hbs.edu/faculty/Publication%20Files/09-005.pdf (accessed May 6, 2013).

[7] "Science and Engineering Indicators 2012," available at: http://www.nsf.gov/statistics/seind12/c3/c3s4.htm#s4 (accessed May 6, 2013).

[8] NAFSA: Association of International Educators, "The Economic Benefit s of International Students to the U.S. Economy Academic Year 2011 – 2012", 2012, available at: http://www.nafsa.org/_/File/_/eis2012/USA.pdf (accessed May 6, 2013).

[9] Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," 2011, available at: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (accessed May 6, 2013).

- In September 2012, engineer Sixing Liu stole files detailing the guidance systems for missiles, rockets, target locators and unmanned aerial vehicles from a division of L-3 Communication.

- In March 2012, former DuPont scientist Tze Chao pleaded guilty to providing trade secrets to companies he knew were controlled by the government of China.

- In February 2010, former Rockwell and Boeing engineer Dongfan Chung was sentenced to prison for stealing restricted technology and trade secrets related to the Space Shuttle program and the Delta IV rocket.[10]

China is not the only threat. Former Cold War adversaries in Russia view the United States as a strategic competitor and are also aggressive and capable collectors of U.S. economic information and technology.[11] In his book *Comrade J: The Untold Secrets of Russia's Master Spy in America After the End of the Cold War*, Peter Earley chronicles the activities of Sergei Tretyakov, the head of political intelligence for Russia's foreign intelligence service, the SVR [the Sluzhba Vneshney Razvedki], in New York City from 1995-2000. "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," Earley quoted Tretyakov as saying.[12] Tretayakov also recounted an instance when an SVR agent provided unreleased medical data and proprietary information based on medical patents held by U.S. companies. While the underlying research reportedly cost the U.S. government $40 million to fund, the SVR agent refused to accept any payment.[13]

Terrorists can also clandestinely acquire the advanced technological information or materials needed to build a nuclear, biological, chemical or radiological weapon. In February 2011, Khalid Ali-M Aldawsari, a Saudi student studying chemical engineering at Texas Tech University, was charged with attempting to use a weapon of mass destruction. A journal found at Aldawsari's residence described how he sought and obtained a particular scholarship because it allowed him to come directly to the United States and helped him financially, which he said "will help tremendously in providing me with the support I need for Jihad."[14]

[10] Ibid.
[11] Ibid.
[12] Cited in Daniel Golden, "American Universities Infected by Foreign Spies Detected by FBI," Bloomberg, April 08, 2012, available at: http://www.bloomberg.com/news/2012-04-08/american-universities-infected-by-foreign-spies-detected-by-fbi.html (accessed May 6, 2013).
[13] Peter 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), p. 274.
[14] U.S. Department of Justice, Press Release: "Texas Resident Arrested on Charge of Attempted Use of Weapon of Mass Destruction," February 24, 2011.

Mechanisms for Oversight

Screening of Foreign Students and Scholars

The United States has allowed foreign students to study in U.S. institutions on temporary visas since the Immigration Act of 1924.[15] Each year, hundreds of thousands of international scholars and students participate in education and exchange programs at American colleges and universities. In the 2011-2012 school year, 764,321 students from abroad were enrolled at U.S. colleges and universities.[16] A visa system that is secure, timely, efficient, transparent and predictable is the first line of defense and permits both scientific exchange and enhances national security.

Export Control Regulations

The federal government controls the flow of information and materials through export control and arms trafficking regulations. Specifically, the Department of Commerce implements the Export Administration Regulations (EAR), which restrict the export of "dual-use" goods and technology – items with both civilian and military applications – found on the Commerce Control List. The Department of State implements the International Traffic in Arms Regulations (ITAR), which regulate the export of defense items and munitions enumerated on the U.S. Munitions List (USML).

Technology export controls are vital to U.S. security and competitiveness, but they have also challenged the ability of industry, laboratories and academia to engage international partners. Many have argued that the regulations are outdated and unnecessarily complicated. In 2009, former National Security Advisor Brent Scowcroft and Lockheed-Martin CEO Norm Augustine co-chaired a National Academies committee which produced a report titled "Beyond 'Fortress America:' National Security Controls on Science and Technology in a Globalized World." The report bluntly stated: "The national security controls that regulate access and export of science and technology are broken. As currently structured, many of these controls undermine our national and homeland security and stifle American engagement in the global economy, and in science and technology."[17]

In August 2009, the Obama Administration launched a comprehensive review of the U.S. export control system with the ultimate aim of creating a unified system with one licensing agency, one control list, a single enforcement coordination agency and an integrated information technology

---

[15] U.S. Library of Congress, Congressional Research Service, "Monitoring Foreign Students in the United States: The Student and Exchange Visitor Information System (SEVIS)," by Alison Siskin, RL32188, (Washington, DC: Office of Congressional Information and Publishing, January 14, 2005).

[16] Institute of International Education, "Open Doors 2012: Report on International Educational Exchange – Fast Facts," available at: http://www.iie.org/en/Research-and-Publications/Open-Doors (accessed May 6, 2013).

[17] Committee on Science, Security, and Prosperity; Committee on Scientific Communication and National Security; National Research Council, "Beyond 'Fortress America': National Security Controls on Science and Technology in a Globalized World," (Washington, DC: National Academies Press, 2009), p. ii.

(IT) system.[18] As of April 2013, the Department of State and the Department of Commerce had issued the first set in a series of final rules that redefine how the U.S. government protects sensitive technologies and regulates exports of munitions and commercial items with military applications.[19]

Classification

Classification is the most appropriate mechanism when it is required that certain information be maintained in confidence in order to protect American citizens and national security. NSDD-189 states:

> "It is also the policy of this Administration that, where the national security require control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: a) determining whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts, or cooperative agreements for potential classification. No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes."[20]

Proper use of the established national security information classification system will allow for clear distinctions between classified and unclassified research, help eliminate uncertainties among scientists and officials responsible for enforcing regulations and better prevent the loss of sensitive information.

[18] U.S. Library of Congress, Congressional Research Service, "The U.S. Export Control System and the President's Reform Initiative," by Ian F. Ferguson and Paul K. Kerr, R41916, (Washington, DC: Office of Congressional Information and Publishing, January 11, 2013).
[19] Department of State, "Export Control Reform: First Final Rules Mark Major Milestone," available at: http://www.state.gov/r/pa/prs/ps/2013/04/207597.htm (accessed May 10, 2013).
[20] NSDD 189, *supra*, note 1.