House Science Committee, Subcommittee on Oversight
Hearing on "Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation while Protecting Critical Information"
May 16, 2013

Michelle Van Cleave
Answers to Questions for the Record to Dr. Broun

1a. In as much detail as you can provide without compromising classified information, what actions are the counterintelligence and law enforcement communities taking to detect, deter and neutralize intelligence threats to the science and technology communities?

From my past experience, I can tell you that foreign intelligence threats to the U.S. science and technology base are a serious concern to U.S. counterintelligence and law enforcement. Security awareness training is routinely practiced at federal laboratories and among cleared personnel. Technology control laws and regulations are properly enforced. The FBI maintains outreach programs to bring threat information to U.S. business and industry and academia engaged in S&T activities that may be of interest to adversaries or competitors.

For a more complete answer, I would urge the Committee to request a briefing from the incumbent National Counterintelligence Executive. I think the Committee will find that, under the current case-by-case business model, counterintelligence and law enforcement are performing at very high levels of professionalism, under the resource constraints imposed by competing national priorities. It is the business model itself that is the limiting factor, as I explain below.

1b. Do we have a comprehensive strategy of our own to counter China's robust, nationally directed strategy to steal American technology and ingenuity?

No. In the first place, to my knowledge there is no national strategy governing our overall relations with China. Nor do we have broad policy guidance to integrate the instruments of state power – intelligence, law enforcement, diplomatic, economic, military and others – to address Chinese S&T acquisition activities.

In the second place, the U.S. counterintelligence enterprise is not postured globally to detect, deter or neutralize the intelligence activities of China or any other foreign power, or to execute strategic counterintelligence operations. Indeed, we know surprisingly little about adversary intelligence services relative to the harm they can do. Under the current business model, there is no national level system that enables the integration and coordination of the diverse activities of U.S. counterintelligence to achieve common strategic objectives. No single entity has a complete picture to provide warning of possible foreign intelligence successes, to support operations, or to formulate policy options for the president and his national security leaders.

1c. If not, what more should we be doing?

In my opinion, it would be extremely helpful to have a clear national strategy to bring coherence to U.S. policies and programs concerning China. If President Obama follows the path of his predecessors and fails to issue one, the Congress could undertake to do so at least for the purpose of providing standards against which authorization, appropriations and other legislative matters might be measured. For example, here is a sample bill, which I offer for the Committee's consideration:

H.Res. _____ U.S. RELATIONS WITH CHINA

Setting forth a strategic policy framework for U.S. relations with the People's Republic of China to guide matters before the House of Representatives.

Whereas

Relations between the United States and China will be key to Americans' peace and prosperity for decades to come, but successive U.S. administrations have failed to provide a guiding strategy or framework for U.S. policy toward China, inviting conflicting and internally contradictory policy pursuits;

There is a time-honored bond of friendship between the American and Chinese peoples, but the Government of China has continued to oppress the people of China by denying basic human rights, such as freedom of speech and religion, and suppressing minority groups;

The PRC has become a formidable economic power and a significant trading partner to the betterment of American consumers and businesses who enjoy access to decent quality, low-cost Chinese goods, but the PRC has repeatedly violated WTO rules and U.S. export controls laws, engaged in industrial and cyber espionage, and infringed U.S. patent and other intellectual property rights;

The U.S. has a historic commitment to freedom of the seas, strategic partnerships with Japan and Taiwan, strong defense alliances and cooperation with regional allies, but the PRC is pursuing a rapid military buildup that challenges U.S. defense capabilities and the stability and security of friends and allies in East Asia and the Pacific.

Successive U.S. administrations have worked to achieve more transparency and confidence in China's relationship with the U.S. and Chinese activities worldwide, but China continues to regard the United States as its principal strategic adversary and to expand its military, intelligence and economic reach globally, including a significant intelligence presence within the United States.

Therefore be it Resolved, that House of Representatives shall measure such bills and resolutions as may be considered by this Body or its Committees of jurisdiction concerning or affecting U.S. relations with China against these guiding strategic U.S. objectives:

To sustain and deploy clear and unambiguous defense and intelligence capabilities to resist any resort to force or other forms of coercion that would jeopardize the peace and stability of the Asia/Pacific region or the security of U.S. friends and allies;

To exert internal pressure on the Chinese government to support liberalization, transparency, democratization and human rights;

To engage with the Chinese government to eliminate, on the basis of strict reciprocity, outstanding disagreements;
To convey clearly to Beijing that responsible behavior on their part will create the possibility for a genuine partnership to our mutual advantage, while any unacceptable behavior will incur costs that would outweigh any gains;

To prevent the transfer of technology, intellectual property or equipment that would make a substantial contribution to Chinese military capability; and

To ensure a robust economy and self-sufficiency at home as the surest means of providing leverage to deal with China on all fronts.

Resolved further, that any and all Authorization or Appropriations Bills reported to the Full House for consideration shall be accompanied by a Report setting forth their compliance with these principles.

The U.S. government also needs to establish a strategic counterintelligence program to integrate and coordinate U.S. counterintelligence assets to achieve strategic objectives – not to supplant current case-by-case operations but to add a new strategic dimension to the national CI enterprise. While the creation of such a program goes beyond the jurisdiction of this Committee, the Oversight Subcommittee might consider addressing their concerns over the vulnerability of U.S. S&T to the House Permanent Select Committee on Intelligence (HPSCI) for follow up. I am unaware of a precedent for a sister Committee of the House referring a matter to the HPSCI, but the logic behind its creation suggests that the Chairman should be receptive to such a request.

2) As suggested by the title of the hearing, our ultimate goal is to develop sensible policies that balance scientific cooperation and security. How would you define sensible policies vs. bad policies? Further, how would we know what constitutes an appropriate balance between scientific cooperation and security?

As I see it, in this context security is a risk management function that exists to support the goals of scientific cooperation. Part of the answer to developing sensible policies includes educating S&T personnel about security in order to give them a true understanding of the several security disciplines, how they work and why they matter, rather than just handing them a list of rules to follow.

Secondly, if we had better insights into foreign intelligence threats and better means of dealing with those threats (i.e., more effective counterintelligence programs and capabilities), then the risks associated with international S&T cooperation would go down. The former Administrator of NASA Mike Griffin and I co-authored an article on the subject of US-Chinese cooperation in space, which speaks to this question. I am providing the text so that it might be included in the record:

The Washington Times

GRIFFIN & VAN CLEAVE: Working with China opens door to espionage

Cooperating in space: Time for a timeout

By Michael Griffin and Michelle Van Cleave July 7, 2011

It was an awkward moment, to say the least. Testifying before a House Appropriations subcommittee, President Obama's science adviser, John P. Holdren, was describing the Obama administration's ongoing discussions with China to develop joint space projects.

Problem is, a law Mr. Obama had signed just weeks before prohibits NASA or Mr. Holdren's Office of Science and Technology Policy (OSTP) from engaging in any bilateral activities with China.

When challenged ("Do you understand the meaning of the word 'prohibits'?") Mr. Holdren asserted on advice of counsel that the president was construing the law as consistent with his inherent constitutional authority to conduct negotiations (lawyer-speak for "You can't tell us what is off limits").

Mr. Holdren may pay the price (literally) for this novel interpretation. Now Frank R. Wolf, chairman of the subcommittee on commerce, justice, science and related agencies is threatening to force compliance with the law by cutting OSTP's budget when his subcommittee meets today to mark up next year's appropriations bill.

Leaving aside the "who's-in-charge" issue, the larger question is: Is this a good law or a bad law?

As the former head of NASA and the first to visit China, and the former head of U.S. counterintelligence, we might be expected to reach different answers. Yet we are both in the realist camp. There are two schools of thought about space cooperation with China, each with its own self-fulfilling prophecy:

- The Chinese are determined to steal our technology and get ahead militarily at our expense, so any cooperative space projects are a lose-lose for us. (The national security realists.)
- Chinese espionage will succeed no matter what we do, so we might as well get what we can out of cooperative projects. (The science and technology "realists.")

We think both of these views are overly simplistic.

As America prepares to box up the last space shuttle for museum display, China is on a trajectory of explosive growth in space - under a highly disciplined veil of secrecy. We have precious few insights into what the Chinese are doing or why. Based on our experience with the Soviets during the Cold War and with Russia since, we think carefully managed cooperative space projects - not putting partners into the critical path, just selective joint efforts on interesting things - could be the single best window into Chinese plans and capabilities in space.

At the same time, the Chinese have a far-reaching, multilayered program for illicit technology acquisition from the United States. They 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.

We want to open channels that allow the possibility that in the long run, a potential adversary can become a partner and ally. Joint space projects characterized by transparency, reciprocity and mutual benefit can be an excellent way to begin. Is it possible to manage the inherent risks while pursuing our larger goals?

If we had an effective counterintelligence capability to identify and disrupt Chinese collection activities, this would be an easier call. Timely tripwires that signal when the other side is stepping across the line would enable us to manage the risk of close interaction and gain the advantage of rare insights into China's space program. Unfortunately, U.S. efforts to build such a strategic capability against foreign intelligence threats have fallen by the wayside, while Chinese espionage continues to grow.

We believe the United States is paying an opportunity cost by walking away from possible joint space projects with China, but without a more robust counterintelligence capability, we stand to lose more than we would gain. Nor does it make sense to venture into cooperative activities that may contribute to China's military modernization or global strategic ambitions.

The statutory prohibition against bilateral space projects wisely puts the brakes on a downhill rush to engage with the Chinese. In the absence of a larger strategy guiding policy and programs on China, it is unclear whether cooperative space projects would advance or hinder U.S. interests. The Obama administration should use this timeout to take stock and then return to Congress with a coherent approach to space cooperation with China that is more than a raw assertion of the president's authority to conduct foreign affairs as he may please.

Michael Griffin was the administrator of NASA under President George W. Bush. Michelle Van Cleave was the national counterintelligence executive under President Bush and assistant director of the White House Office of Science and Technology Policy under Presidents Reagan and George H. W. Bush.

3) I understand that certain countries like China, Russia, Iran and North Korea require additional security because of what we know about their interests and attempts on our technologies and information. Keeping that in mind, how do we implement policies that protect our assets while avoiding accusations of profiling?

China's intelligence services routinely target overseas Chinese for recruitment; they are the ones doing the profiling, not the U.S. government. I am unaware of the other countries cited following similar practices.

4) Do you have any recommendations on what steps our academic institutions and labs can take to defend from attacks directed specifically at our cyber infrastructure, and can we share or apply those suggestions to American businesses and government agencies which are constantly bombarded by cyber-attacks from foreign nationalists?

Academic institutions and research facilities can begin by understanding that they are targets for foreign collection, and protect their information systems accordingly. Business and industry have additional commercial incentives for protecting their proprietary information, and our entrepreneurial society is responding by provided ever more and better cybersecurity solutions. The legal system and the insurance industry also have an increasingly significant role to play in allocating risk for cyber-related losses ("who pays, protects"). But history has shown that the offense will always have an advantage over the defense, which means that security measures alone will never be enough. At the national level, the United States also needs robust capabilities to identify, assess and defeat cyber operations directed against us.

5) The classification system is an important tool to keep truly sensitive information safe and secure. But overclassification can jeopardize national security by preventing federal agencies from sharing information internally, with other agencies or with non-governmental organizations. How can we prevent overclassification and ensure that classifiers comply with existing criteria for classifying documents?

One of the most-cited lessons coming out of the September 11 terrorist attack was a failure to "connect the dots" – *i.e.,* to bridge what was known from foreign intelligence sources with law enforcement or other domestic information about potential threats. The hurried conclusion was "we need to share more" when the conclusion should have been "we need dedicated, discrete intelligence fusion capabilities" as well as assigned responsibilities to take action. As a result, the current system for protecting intelligence sources and methods and other sensitive national security information has become distorted in two ways.

First, the move from a standard of "need to know" (pre-9/11) to "need to share" (post 9/11) has resulted in an exploding population of people with security clearances, overwhelming the resources of the personnel security system to keep up. I have seen statistics showing that 5 million people – one in every 50 American adults – now hold security clearances. Security challenges are close to impossible to meet with a population that large; at best, there will serious gaps, indiscriminate enforcement and escalating risk. Among other things, we see the

emergence of destructive individuals like Bradley Manning and Edward Snowden -- bit players on a quest to prove their own importance, taking advantage of their overly broad access to sensitive information.

Second, all of the incentives are to "dumb down" classification standards, *i.e.,* to classify more and broader categories of information as "secret," reserving "top secret" for what was previously "secret." In turn, more people need security clearances to access mundane "secret" information to do their jobs, putting them in line for moving up the ladder to higher levels of clearance. Along the way, it's not difficult to imagine how individuals who see relatively innocuous information labeled "secret" may acquire a casual disregard for the weighty responsibilities that adhere in protecting information which, if disclosed, in fact would cause serious harm to the nation's security.

A far better approach would be to decide what truly needs to be protected and to protect that extremely well, including returning to clear "need to know" standards that can be responsibly implemented while facilitating the operations they exist to support.