Responses to Dr. Broun's Questions

1. **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?**

It seems to me that the emphasis should be on actual security programs, i.e. the real-world application of our laws and policies. Just as in good business practice, security programs need to be well thought out but then continuously improved or discontinued based on periodic data-driven evaluation. Indeed, a National Academies committee co-chaired by former Secretary of Defense William Perry and myself addressed this issue. Our recommendations included a framework for security programs that specifically included eight elements:

a. Agency Competency
b. Well-defined Purpose
c. Measured Effectiveness
d. Appropriate Authorization
e. Appropriateness of Data
f. Redress for those inappropriately affected
g. Periodic Assessment
h. Appropriate Oversight.

This framework was developed especially for information-based programs, such as those making headlines today. However, I believe the key thing is periodic, structured, and serious evaluation of the effectiveness of security programs that weighs the real (not theoretical) benefits and costs. In this case the "benefits" would be detection or disruption of damage to our security and/or economy, and the "costs" would be disruption or damage to the our scientific and technological advancement and leadership and economic opportunities.

2. **I understand that certain countries like China, Russia, Iran and North Korea require additional scrutiny 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?**

To the greatest extent possible, we should treat every individual who has been admitted to the U.S. to study or perform R&D the same. Sadly, Timothy McVeigh was just as evil, and his acts just as horrendous, as those of any foreign terrorist might be. Critical industrial IP and truly essential security information should be protected from domestic criminals and noncitizens alike. The criteria should be the same.

On the other hand, when things like cyber intrusions occur, we must counter where the source wherever it is. If the source is dominantly in one of the countries mentioned in your question, I don't consider that to be profiling. At the same time, we don't want to blindly shut our doors. Many of our best researchers and entrepreneurs have come here from China, Russia, and Iran.

3. **Do you have any recommendations on what steps our academic institutions and labs can take to defend 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 nationals?**

This is a very important matter, but the specific answer to your question is a technical matter beyond my expertise. However, there are a couple of points I would like to make:

First, cyber attacks and intrusions are simply facts of modern life. They can be, and are, effectively carried out by individuals with widely varying motivations as well as by state actors. Second, for the foreseeable future, there will be a continuous escalation in the nature and sophistication of such attacks, and therefore, countermeasures must also advance dynamically; there will be no one-time fix.

There is a lot of cyber security expertise in our universities and in small companies. My colleagues and I would be glad to point your staff toward some of these if that would be helpful.

4. **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 classifiying documents?**

I believe that we have serious problems of overclassification and mission creep. According to a 2011 report by the Director of National Intelligence, over 4 million people held security clearances, and of this group, 1.2 million held Top Secret or TS/SCI clearances. Beyond that, there is an unnecessary and confusing proliferation of categories like "sensitive but unclassified," and an overly broad and badly outdates export control regime.

In a technological world that moves as fast as today's, it seems very clear that we need to narrow the scope of classification by narrowing the criteria which classifiers apply to better represent those things that are truly critical to our security. In my view, it would be good practice to do periodic post audits of representative samples of classified materials and activities to honestly assess whether the initial decision to classify was justified in retrospect. The system could then be continuously improved and narrowed over time.

My experience observing and working with private industry suggests that they are much better and more focused than the government about what IP really needs to be protected. Their domains of interest are often quite different than that of the national security community, but I think the federal sector could learn from the business sector.

Finally, especially in the commercial context, I continue to believe that it truly is more important to fill our proverbial bucket of new knowledge and technology than to obsessively plug leaks. If we can reduce

unnecessary bureaucracy and security, we can get new things into the hands of our entrepreneurs to create jobs and get them to market. Speed is really important today.