

## Recent Press Releases

### **Thune Statement on Cybersecurity Hearing**

*Republican Press Office - (202) 228-5381*

*Jul 25 2013*

**WASHINGTON, D.C.** — U.S. Senator John Thune (R-SD), Ranking Member of the Senate Committee on Commerce, Science, and Transportation, delivered the following prepared remarks at today's "The Partnership Between NIST and the Private Sector: Improving Cybersecurity" full committee hearing:

Thank you, Mr. Chairman, for holding this hearing, and for your continued leadership on cybersecurity. You brought this critical issue to the fore, and you have been steadfast in your commitment to addressing the problem. No one can deny the serious threat we are confronting in cyber space. Almost daily, we learn of new cyber threats and attacks targeting our government agencies and the companies that drive our economy. We must find solutions that leverage the innovation and know-how of the private sector, as well as the expertise and information held by the federal government. And, given the escalating nature of the threat, we should look for solutions that will have both an immediate impact and that will remain flexible and agile into the future.

In keeping with that task, in March, this Committee held a joint hearing with the Homeland Security and Governmental Affairs Committee not long after the president issued his Cybersecurity Executive Order in February. Today, we are here to examine the National Institute of Standards and Technology's (NIST) implementation of that portion of the Executive Order pertaining to the cybersecurity partnership between the private sector and the federal government to improve best practices in cybersecurity. The feedback we have heard from many in industry regarding NIST's process has been fairly positive so far.

We are also here to examine the legislation that Chairman Rockefeller and I have introduced, after soliciting feedback from industry stakeholders and our colleagues. I think this bill strikes the proper balance to ensure that what develops is industry-led and a true partnership between NIST and the private sector. It also ensures that NIST's involvement, and this process, are both ongoing, in order to maintain the flexibility and continued innovation that is necessary to meet such a dynamic threat.

Our proposed legislation also includes needed titles to improve research and development. We should not underestimate the value of R&D. As I have mentioned previously, I'm proud to note that South Dakota's own Dakota State University is one of only four schools in the nation designated by the National Security Agency as a Center of Academic Excellence in Cyber Operations. Other titles of our bill improve education and workforce development, as well as cybersecurity awareness and preparedness.

I am pleased that our offices worked with industry, fellow Senate colleagues, and other stakeholders to solicit and incorporate their feedback in crafting this legislation, and will continue to do so as we move forward. By following regular order in the committees of jurisdiction, we hope to avoid the legislative impasse from last congress and ultimately enact legislation that will make real improvements to our nation's cybersecurity. Our hearing witnesses today include the Director of NIST, and representatives from the private sector who can provide this committee with their perspectives on how the current NIST process is developing. I look forward to hearing whether our legislation is a step in the right direction to provide a partnership that is truly voluntary and industry-led.

I am also pleased that the Chairman and I both recognize that an essential component of cybersecurity is strong information sharing regarding threats. Such sharing should occur both between government and industry, and among private sector actors, with strong liability protections. It is our hope that our colleagues on the Senate Intelligence Committee will be successful in crafting bipartisan, consensus legislation that achieves these goals. As the Chair of the House Intelligence Committee has said, according to intelligence officials, allowing the government to share classified information with private companies could stop up to 90 percent of cyber attacks on U.S. networks. It is also our hope that the Senate Homeland Security Committee can similarly work in a bipartisan fashion to make needed improvements to the Federal Information Security Management Act in order to better secure our federal networks. If our committees can work to produce complementary consensus legislation, that will be a significant step forward in this area.

Again, I thank the Chairman for holding this hearing and I thank all of the witnesses for being here, and I look forward to hearing your testimony.

###