Testimony

of Dorothy Coleman
Vice President
Tax, Technology and Domestic Economic Policy
National Association of Manufacturers

before the Senate Committee on Commerce, Science and Transportation

on "The Partnership Between NIST and the Private Sector: Improving Cybersecurity"

Thursday, July 25, 2013

COMMENTS FROM THE NATIONAL ASSOCIATION OF MANUFACTURERS

BEFORE THE SENATE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION

JULY 25, 2013

Chairman Rockefeller, Ranking Member Thune and members of the committee, thank you for the opportunity to appear today to testify on behalf of our nation's manufacturers on "The Partnership Between NIST and the Private Sector: Improving Cybersecurity."

My name is Dorothy Coleman, and I am the vice president of tax, technology and domestic economic policy at the National Association of Manufacturers (NAM), the nation's largest industrial trade association, representing small and large manufacturers in every industrial sector and in all 50 states. We are the voice of 12 million manufacturers in America.

The NAM has enjoyed a close working relationship with the committee for a number of years. Mr. Chairman, we appreciate your unwavering support for the Hollings Manufacturing Extension Partnership, which has proved invaluable for small manufacturers in West Virginia and around the country working to develop the next breakthrough manufacturing technology. Thank you, too, for your leadership on spectrum issues, which are critically important to the many manufacturers that use wireless technology in their businesses.

Ranking Member Thune, the NAM and our members have worked closely with you on multiple issues. You have been a strong advocate for the close to 40,000 manufacturing employees in South Dakota on both tax and trade issues. We look forward to continuing our working relationship with you on cybersecurity and the other legislative priorities for manufacturers.

Cybersecurity has been a focus of this committee in recent years. On behalf of our nation's manufacturers and all those who want to ensure the protection of our critical assets and intellectual property (IP) and to work together with the government to achieve this goal, I am pleased to testify on the Cybersecurity Act of 2013 and to discuss the partnership between the National Institute of Standards and Technology (NIST) and the private sector.

Overview

Manufacturing remains an important economic force in the United States, representing 12 percent of the U.S. economy. Nonetheless, despite the critical role the industry plays in the economy, taxes, legal costs, energy prices and burdensome regulations make it 20 percent more expensive to manufacture in the United States than in any other country.

The NAM's *Growth Agenda: Four Goals for a Manufacturing Resurgence in America* is a comprehensive plan to address these challenges, unleashing the economy and manufacturing's outsized multiplier effect. The *Growth Agenda* makes the case for pro-growth polices to ensure that:

- The United States will be the best place in the world to manufacture and attract foreign direct investment;

- Manufacturers in the United States will be the world's leading innovators;

- The United States will expand access to global markets to enable manufacturers to reach the 95 percent of consumers who live outside our borders; and

- Manufacturers in the United States will have access to the workforce that the 21st-century economy demands.

Manufacturers recognize that we face very specific challenges in achieving these goals. In particular, in pursuing our goal to be the world's leading innovators, our industry faces constant threats from nefarious actors in cyberspace attempting to access our IP and operations unlawfully. These threats endanger our continued economic growth and safety of our citizens.

Thus, the NAM believes that we need to develop appropriate general and industry-specific best practices for improved cybersecurity. In formulating cybersecurity policy, we support a public–private partnership that draws on industry best practices.

The cybersecurity debate has moved forward significantly this year, and the business community has the leadership of you, Mr. Chairman, and Ranking Member Thune to thank for that. Your bill represents a sensible, bipartisan, non-regulatory approach to an issue of utmost importance to the manufacturing industry. Manufacturers support creating an industry-led, voluntary standards development process, strengthening the cybersecurity research and development strategy inside the federal government, creating a high-skilled cybersecurity workforce and raising public awareness of cyber threats.

The introduction of this bill has also effectively signaled to the business community and to your Senate colleagues the importance of moving this issue forward. There are a number of additional issues that other committees need to debate, but we are pleased with the steps you have taken.

Manufacturers and Cybersecurity

Manufacturers are entrusted with vast amounts of data through their comprehensive and connected relationships with customers, vendors, suppliers and governments. They are responsible for securing the data, the networks on which the data run and the facilities and machinery they control at the highest priority level.

In addition, manufacturers are the owners, operators and builders of our nation's critical infrastructure. They manufacture and use the temperature controls regulating the grain silos that store our nation's food supplies. They build and manage the systems operating the traffic signals that govern the rules of the road. Manufacturers make technology products ranging from nanoscale electronic devices to fighter jets. They build and run the energy plants that power our homes and businesses and the heavy machinery exploring the oil and gas fields that make America competitive.

In addition, manufacturers leverage technology to design, produce and deliver these products. Technology is also used to manage, monitor and secure key facilities and products, including trade secrets and patents.

These products, controls, systems, patents, trade secrets and all other tools that differentiate manufacturers in the United States from their competitors are the envy of the world. The movement of design, collaboration and information that helps drive this innovation almost exclusively online has created a new vulnerability: exposure to cyber thieves that are constantly

attempting to penetrate networks to steal this IP. This illegal activity allows bad actors to replicate products and designs and disrupt business activity and critical infrastructure.

The stakes are high. What was once only the concern of businesses' IT departments has now become an important issue throughout manufacturing facilities, large and small. Leaders of manufacturing enterprises know they have to secure their networks, their controls and their data. In fact, in a recent NAM membership survey, 96 percent of respondents said they have ongoing efforts to strengthen their information technology networks and protect their IP to reduce their risk. More than 90 percent have upgraded their IT assets, and more than half have hired outside cybersecurity experts.

Manufacturers know the economic security of the United States is related directly to our cybersecurity. Given that our economic security is critical to our national security, manufacturers are leaders in cyber defense and are working constantly to ensure their companies, products and customers are secure.

Cybersecurity Policy

During the cybersecurity debate in recent years, the NAM has been clear on what actions we believe the government should take to address current cyber threats most effectively. We have communicated our priorities to leaders in both the House and Senate and to the White House. I am pleased to share those with you again today, and I applaud you for addressing a number of these issues over which your committee has jurisdiction.

NAM members value the strong partnership they have with the public sector and believe that partnership should extend to cybersecurity efforts. The NAM encourages the federal government to advance cybersecurity preparedness through increased collaboration and coordination with the private sector.

In particular, manufacturers' top priority is allowing the voluntary sharing by the public and private sector of real-time threat information to allow manufacturers to better protect themselves from cyber threats. In contrast, under current law, the government is prohibited from sharing sensitive cyber-threat information with the private sector. Manufacturers are hesitant to share information with the government due to liability uncertainty and exposure. Companies also are not permitted to share information freely with their peers.

The NAM supported the Cyber Intelligence Sharing and Protection Act (CISPA) of 2013 (H.R. 624), which the House passed earlier this year. This legislation, if signed into law, will allow the government to share timely and actionable threat and vulnerability information with the private sector. Mr. Chairman, as a member and former chairman of the Senate Intelligence Committee, we encourage you to work with your colleagues on that panel to address the issue of information sharing.

Manufacturers value the privacy of individuals and the need to protect personally identifiable information and civil liberties. We believe that any cybersecurity initiative the federal government undertakes separately or in partnership with the private sector should place a premium on ensuring this information is secure. At the same time, it is important to ensure that any effort does not grant the government any new authority in this realm or give the government the ability to monitor or censor private networks.

Developing a Cybersecurity Standards Framework

The NAM believes that the public and private sector must partner closely to establish the best way to defend against ever-changing cyber threats manufacturers face. We oppose, however, the creation of a static, regulatory-based regime. This approach will not enhance cybersecurity - it will do just the opposite.

The cyber threat that now confronts all entities in both the public and private sector is commonly known as the "advanced persistent threat" or APT. Cyber hackers and thieves are changing their tactics every minute. Manufacturers need the flexibility to pivot quickly and defend against these threats in real time. Any mandatory regulations imposed on manufacturers will be obsolete the day they are published. The time spent complying and adjusting to outdated, burdensome and potentially duplicate regulations will negatively impact manufacturers' ability to protect their key assets.

Rather than develop mandatory regulations, the government should apply to the cybersecurity challenge the public–private partnership model that has been effective in other areas. While the federal government has the resources to facilitate industry-led discussions on how best to defend against the APT, industry officials bring real-world expertise and experience unique to their segment.

In fact, NAM member companies have been on the record in their comments to NIST and in their participation in the cybersecurity framework discussions around the country that implementing any framework should be on a voluntary company-by-company basis. The framework needs to be risk-based, and it must keep pace with ever-changing cyber threats. Most importantly, any threat information the government can share with the private sector will be the most effective way to combat cyber threats.

A one-size-fits-all approach to a standards framework will not be effective. Manufacturers vary in size, come from a cross-section of diverse industry segments, have differing amounts of available resources and are exposed to external actors in different ways. These factors all will play a role in how each manufacturer implements a cybersecurity strategy. Imposing a single regulatory model would result in little or no participation in the framework. Rather, the framework should act more as a guideline and advocate for best practices. The framework must also take into account the global presence of manufacturers and all international markets in which they operate and the related international standards already in place.

The most common theme we have heard from our members is that a number of standards already exist. A major concern is that the creation of any new set of standards—even if they are voluntary—could lead to another regulatory regime and cause even more challenges for manufacturers. Any framework NIST may develop must take into account existing standards already being followed by the private sector.

Cybersecurity Act of 2013, S.1353

The Cybersecurity Act of 2013, S.1353, introduced yesterday addresses many of the challenges described above. Mr. Chairman and Ranking Member Thune, we appreciate your efforts to reach out to all stakeholders to create a balanced approach to reduce the risk of cyber threats to critical infrastructure based on a public–private partnership model.

The legislation would create a national cybersecurity research and development plan to further secure wireless technology, software systems and the Internet, while guaranteeing individual privacy. The legislation would also create cybersecurity modeling and test beds to examine our capabilities and determine our needs. It does all of this while ensuring coordination across the government. We appreciate your efforts to raise the priority of cybersecurity throughout all agencies.

Your bill also would place a priority on developing a high-skilled cybersecurity workforce. Through competitions, challenges and scholarships, it would create incentives to join this growing workforce at a time when our country needs it most. Most importantly, it would assess current skill sets and help determine what more is needed in curriculum and training to ensure we have the workforce we need. Manufacturers are facing a skills shortage in many disciplines, and any effort to close that gap is one we support strongly.

The national cybersecurity awareness and preparedness campaign has been well received by NAM members. Efforts to increase the cyber intelligence and cyber safety of the public and state and local governments will benefit manufacturers as they hire the workers they need and as they operate in their communities.

We have heard the most from our member companies on Title I of the bill, Public–Private Collaboration on Cybersecurity. As I stated earlier in my testimony, the ability to receive real-time threat information remains manufacturers' top priority. This will be the most effective way to combat cyber threats. Manufacturers realize that an ongoing partnership with the federal government—in addition to information sharing—is also important.

In addition, NAM members generally support establishing NIST as a facilitator of industry-led discussions on standards, guidelines and best practices among other efforts to reduce cyber risks to critical infrastructure. Many NAM members are participating in the NIST cybersecurity framework discussions underway. Those sessions have been productive, and our members want the process to continue.

Nonetheless, they have some concerns about this approach. In particular, some companies are concerned that codifying NIST as the facilitator may somehow negatively impact the process, or even worse, give NIST the authority to recommend binding regulations.

It is our understanding that creating new regulations is neither the intent nor the goal of the legislation. We appreciate that this is referenced specifically in the bill, which requires that any recommended standards are voluntary and will not prescribe specific technology solutions, products or services. The legislation is even more specific by citing that any information shared in the standards development process shall not be used to regulate any activity of the sharing entity.

On behalf of the NAM's 12,000 members, this is a point I cannot stress strongly enough—manufacturers will not support any legislation that creates a duplicative regulatory regime that puts undue burdens on manufacturers. We are, therefore, pleased that this legislation prohibits that from happening while at the same time solidifies the public–private partnership in efforts to address an issue of critical importance to our nation.

Conclusion

In our fast-moving, hyper-competitive 21st-century economy, cybersecurity is an issue of increasing importance to the manufacturing industry. The stakes are high for manufacturers and the rest of the business community. Manufacturers' ability to protect their products, processes, facilities and customers is critical for their continued success and the broader economic security of the nation. The legislation the committee is examining today represents a good first step in assisting manufacturers in their ongoing efforts to reduce their cyber risk. Manufacturers must and will continue to drive the process, and a partnership with the government is a key component of the effort. The NAM supports the goals of the legislation and appreciates the committee's efforts to address this important issue. Thank you for the opportunity today to appear before you. The NAM looks forward to working with the committee as the process moves forward.