Business Roundtable℠

300 New Jersey Avenue, NW
Suite 800
Washington, DC 20001

Telephone 202.872.1260
Facsimile 202.466.3509
Website brt.org

Statement Submitted for the Record

U.S. House of Representatives
Permanent Select Committee on Intelligence

John Engler
President
Business Roundtable

February 14, 2013
Hearing on

"Advanced Cyber Threats Facing Our Nation"

Chairman Rogers, I commend you, Ranking Member Ruppersberger, and the distinguished members of this Committee for your continued focus on our nation's cybersecurity preparedness. We applaud you for reintroducing the Cyber Intelligence Sharing and Protection Act (CISPA), which the Business Roundtable supported last year. We highly encourage you to continue to work with your counterparts in the Senate, as well as with the Administration, to ensure this important legislation contains appropriate legal and privacy protections that will pass both chambers of Congress expeditiously and be signed by the President.

The topic of today's hearing is one of the most important issues that Congress will tackle over the coming months. I appreciate the opportunity to share the views of the Business Roundtable on this very important topic. Business Roundtable is an association of chief executive officers of leading U.S. companies with more than $7.3 trillion in annual revenues and nearly 16 million employees. Member companies comprise nearly a third of the total value of the U.S. stock market and invest more than $150 billion annually in research and development – equal to 61 percent of U.S. private R&D spending. Our companies pay $182 billion in dividends to shareholders and generate nearly $500 billion in sales for small and medium-sized businesses annually. Our companies give more than $9 billion a year in combined charitable contributions.

Cybersecurity is a bottom line issue for the more than 200 CEOs of Business Roundtable and a top-level national economic issue because America's strategic information assets are a platform for commerce and economic growth. Our CEOs are responsible for a significant portion of America's critical infrastructure including major portions of the financial services, electric power, oil and gas, telecommunications, defense and chemicals industries. No one has a greater incentive to protect critical systems – or greater knowledge of how to do so – than the businesses that own and operate these critical systems. Information systems constitute the very core of business operations and relationships with customers and suppliers. Protecting our most critical systems is a daily concern that receives constant executive attention.

Increasingly, however, cybersecurity threats are presenting risks to these systems that neither the public nor the private sector can unilaterally protect against. Cybersecurity threats are dynamic and ever-evolving. Some cyber adversaries seek to disrupt critical services and the delivery of goods, while others are stealing sensitive government and corporate information at alarming rates. Cyber adversaries are highly motivated and constantly shifting and changing their methods to accomplish these ends.

With the core of global commerce and safety at stake, our CEOs do not doubt the need for policy and legislative action. From our perspective, the missing piece of effective cybersecurity

is robust, two-way information sharing, with appropriate legal and privacy protections, between business and government. The public-private information sharing partnerships in place today are good but not good enough. They are not sufficiently capable of responding to escalating threats.

Companies have identified several gaps in our current capabilities – many of which this Committee is aware. The current information sharing environment is not supported by strong legal protections to safeguard companies that share and receive cybersecurity information from civil or criminal action. Companies lack formal guidance on antitrust laws, which creates uncertainties for working within and across sectors to share threat information and risk management and mitigation techniques.

Furthermore, there are not nearly enough security clearances. In many cases, only one or two employees are cleared even within very large global enterprises, which create difficulties in communicating problems and acting quickly across global operations. And, without access to timely and actionable threat information, senior corporate leaders can only speculate about which threats are greatest and how to best manage them.

Given the growing cybersecurity threats and gaps in the nation's preparedness, we convened a dialogue among CEOs from a diverse set of economic sectors, including utilities, oil and gas, chemicals, manufacturing and financial services. The result of our efforts is a progressive, consensus-based strategy for improving public-private cybersecurity cooperation. Development of our policy statement was spearheaded by Ajay Banga, President and CEO of MasterCard and Chair of our Information and Technology Committee.

As Mr. Banga recently told the *Wall Street Journal,* "the business of cybersecurity is more like intelligence and counterespionage than security where you put up physical guns and guards." We are calling on the government to become much more sophisticated in the way that it addresses cybersecurity threats. Our strategy lays out an implementation plan for the public and private sectors to jointly address cybersecurity risks. CEOs are committed to doing their part including direct CEO involvement and encouraging board oversight.

Our strategy includes three parts.

First, we support legislation that creates robust, two-way information sharing, with appropriate legal and privacy protections, between government and the private sector to exchange the specific threat information that will allow both government and businesses to better secure the nation's critical assets. The government must create a clear and predictable

legal framework for private sector to private sector and private sector to public sector sharing, with appropriate liability and antitrust protections for those acting within the framework.

Second, the public and private sectors should develop and integrate roles and responsibilities that enable us to systematically work together toward the common goal of protecting our information assets. Business Roundtable supports policies that build upon existing efforts to develop threat-informed risk management and mitigation methodologies to anticipate and respond to the most serious threats. To accomplish threat-informed risk management, an effective partnership should build on existing sector policy coordinating councils and government operations centers, and position senior public and private sector leaders to collaboratively oversee cybersecurity efforts.

Finally, our CEOs are making cybersecurity a top priority by: establishing and resourcing programs to incorporate cybersecurity threat information into corporate risk management; instilling the importance of cybersecurity in the culture of the corporation by setting tone and expectations; assigning responsibilities and developing appropriate metrics; actively monitoring and responding to ongoing risks; and working collaboratively with government on an ongoing basis to improve and advance cybersecurity resilience. In addition, the CEOs of the Business Roundtable are recommending that boards of directors, as part of their risk oversight responsibilities, oversee corporations' risk assessment and management processes, including those applicable to cybersecurity.

Mr. Chairman and members of the Committee, we thank you for the opportunity to share our views. We look forward to working with you to improve the nation's cybersecurity preparedness, protect our economic security and ultimately make our country safer.