June 11, 2014

Michael Daniel
Special Assistant to the President and Cybersecurity Coordinator
The White House
Washington, DC 20500

Dear Mr. Daniel:

Our associations, which represent nearly every sector of the American economy, applaud you and the administration for supporting a dynamic and flexible approach to addressing cybersecurity risk. Your May 22 blog, *Assessing Cybersecurity Regulations*, sends businesses and other stakeholders an important message that the *Framework for Improving Critical Infrastructure Cybersecurity* (the framework) should remain collaborative, voluntary, and innovative over the long term.

Like you, we have invested considerable time and energy toward developing the framework. The National Institute of Standards and Technology (NIST) handled a challenging assignment in ways that ought to serve as a model for other agencies and departments.

We agree with your assessment in the blog that business and government "must build equally agile and responsive capabilities not bound by outdated and inflexible rules and procedures." Our organizations particularly urge independent agencies and Congress to adhere to the dynamic approach advocated by the administration and that is embodied in the nonregulatory, public-private framework.

In addition, industry has demonstrated its commitment to using the framework. Many associations are creating resources for their members and holding events across the country and taking other initiatives to promote cybersecurity education and awareness of the framework. Some examples are listed here. Associations are planning and exploring additional activities as well.

- The American Gas Association (AGA) has hosted a series of webinars on control system cybersecurity and is working with small utilities to develop robust cybersecurity programs. Among other activities, AGA is standing up the Downstream Natural Gas Information and Analysis Center (DNG–ISAC), an ISAC designed to help support the information-sharing interests of downstream natural gas utilities.

- The American Hotel & Lodging Association (AH&LA) has conducted a series of widely attended cyber and data security webinars to assist small, medium, and large hotel and lodging businesses with implementing key information security measures and risk assessments.

- The American Water Works Association (AWWA) has created cybersecurity guidance and a use-case tool to aid water and wastewater utilities' implementation of the framework. The guidance is cross-referenced to the framework.

- Members of the Communications Sector Coordinating Council (CSCC)—made up of broadcasting, cable, wireline, wireless, and satellite segments—have participated in multiple NIST, Department of Homeland Security (DHS), and industry association-sponsored programs, webinars, and panels with future events being planned.

  In addition, the communications sector has roughly 100 cybersecurity experts engaged in the Federal Communication Commission's (FCC's) voluntary Communications Security Reliability and Interoperability Council (CSRIC) to adapt the framework for the segments, focusing on an understanding of shared responsibilities across the ecosystem, the impact on small and medium enterprises, evolving threats, and barriers to implementing specific risk-management capabilities.

- The Electricity Subsector Coordinating Council is working with the Department of Energy (DOE) to develop sector-specific guidance for using the framework. The guidance leverages existing approaches to cybersecurity, including DOE's *Electricity Subsector Cybersecurity Risk Management Process Guideline*, the *Electricity Subsector Cybersecurity Capability Maturity Model*, NIST's *Guidelines for Smart Grid Cyber Security*, and the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection Cybersecurity Standards.

- The mutual fund industry, represented by the Investment Company Institute (ICI), has recently added to its committee roster a Chief Information Security Officer Advisory Committee. The committee's mission is to collaborate on cybersecurity issues and information sharing in the financial services industry and provide a cyber-threat protection resource for ICI members.

- The Information Technology Industry Council (ITI) recently visited Korea and Japan and shared with these countries' governments and business leaders the benefits of a public-private partnership-based approach to developing globally workable cybersecurity policies. ITI highlighted the framework as an example of an effective policy developed in this manner, reflecting global standards and industry-driven practices.

- The National Association of Manufacturers (NAM) has spearheaded the D.A.T.A. (Driving the Agenda for Technology Advancement) Policy Center, providing manufacturers with a forum to understand the latest cybersecurity policy trends, threats, and best practices. The D.A.T.A. Center focuses on working with small and medium-size manufacturers to help them secure their assets.

- The oil and natural gas sector has established a new Oil and Natural Gas Information Sharing and Analysis Center (ONG–ISAC) to provide shared intelligence on cyber incidents, threats, vulnerabilities, and responses throughout the industry.

- The Retail Industry Leaders Association (RILA) has created the Retail Cyber Intelligence Sharing Center (R–CISC), featuring information sharing, research, and education and training. This ISAC enables retailers to share threat data among themselves and receive threat information from government and law enforcement partners.

- The U.S. Chamber of Commerce has launched its national roundtable series, *Improving Today. Protecting Tomorrow*™, recommending that businesses of all sizes and sectors adopt fundamental Internet security practices.

As you note in your blog, NIST and multiple stakeholders produced a smart framework that stakeholders are proud of. But more work lies ahead. We look forward to working with policymakers to ensure that preexisting regulations are harmonized with the collaborative and voluntary nature of the framework. Businesses also seek the enactment of information-sharing legislation to achieve timely and actionable situational awareness to improve our detection, mitigation, and response capabilities.

We share your commitment to protecting America's business community and enhancing the nation's resilience against an array of physical and online threats. Government and business entities need to leverage the framework to strengthen collective resilience and security and make ongoing improvements.

Our organizations look forward to working with you and your colleagues to build on the progress that we—industry and government—have made together.

Sincerely,

Airlines for America
American Chemistry Council
American Fuel & Petrochemical Manufacturers
American Gas Association
American Hotel & Lodging Association
American Petroleum Institute
American Water Works Association
ASIS International
Business Software Alliance
CTIA–The Wireless Association
Edison Electric Institute
Information Technology Industry Council
The Illinois Chamber of Commerce
National Association of Manufacturers
National Business Coalition on E-Commerce & Privacy
National Cable & Telecommunications Association
NTCA–The Rural Broadband Association
Retail Industry Leaders Association
Security Industry Association
Software & Information Industry Association
Telecommunications Industry Association
United States Telecom Association
U.S. Chamber of Commerce