April 17, 2012

The Honorable John Boehner
Speaker
U.S. House of Representatives
Washington, DC 20515

The Honorable Nancy Pelosi
Minority Leader
U.S. House of Representatives
Washington, DC 20515

Dear Speaker Boehner and Minority Leader Pelosi:

The strength of our free enterprise system is directly tied to the prosperity and security of our interconnected world. Cyberspace has become a bulwark of the global economy, with businesses of all sizes increasingly dependent on it for their day-to-day operations. Yet, while innovative technologies help businesses achieve great efficiencies and run our vital infrastructures, we have also seen nefarious global actors—including organized criminals, hacktivists, industrial spies, and foreign governments—take inappropriate advantage of a cyber environment that is open and welcoming to users.

As the House Cybersecurity Task Force recognized this past fall, our organizations are keenly aware of cyber threats to U.S. national and economic security. Private sector members own and operate the vast majority of the systems and assets that are subject to these threats and, therefore, have the greatest incentive to manage and defend against them. At the same time, there is widespread agreement that the protection and resilience of these systems and assets require the public and private sectors to work together, particularly when it comes to greater sharing of information. While personal privacy must be adequately guarded, improved information sharing should aim to enhance situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats.

As House leadership considers what measures are taken up on the floor as early as the week of April 23, we urge lawmakers to focus on the following policy principles and opportunities:

- **Improve information sharing and liability protections:** Our organizations support legislation that would put timely, reliable, and actionable information into the hands of business owners and operators so that they can better protect their systems and assets against the increasing threat of cyber attacks. Legislation should support existing information-sharing and analysis organizations and incorporate lessons learned from pilot programs undertaken by critical infrastructure sectors. Both offer complementary, demonstrated models for enabling the government to share cyber threat information with the private sector in a trusted, constructive, and actionable manner without creating burdensome regulatory mandates or new bureaucracies.

  In addition, businesses need certainty that threat and vulnerability information voluntarily shared with the government would be provided safe harbor and not lead to frivolous lawsuits, would be exempt from public disclosure, and could not be used by officials to regulate other activities. We are committed to working with lawmakers and staff to

ensure that the information-sharing process includes privacy and civil liberties safeguards.

- **Enhance national cybersecurity research and development (R&D):** Congress should leverage public-private partnerships to create a cybersecurity R&D plan that supports national priorities and includes a practical road map for implementation, such as transitioning the benefits of research into operational environments and growing the pool of cybersecurity expertise and talent that both the public and private sectors can tap.

- **Reform the Federal Information Security Management Act of 2002 (FISMA):** There is a strong need to harmonize information security programs across civilian government agencies. An updated FISMA would help the government take advantage of rapidly changing technology capabilities that would enable a shift from a "snapshot-in-time" approach to information security to a truly risk-based approach, where threats are proactively countered based on continuous monitoring of networks and system activity. Above all, the government needs to lead by example and work toward securing its own computers and information systems.

- **Heighten public awareness and education:** Good cyber "hygiene"—or taking relatively simple behavioral precautions, such as keeping antivirus software up to date and backing up files—can reduce a significant percentage of cyber risks to information networks. Our organizations recommend following the example of government and industry mobilization in 2009 to halt the spread of the H1N1 flu virus. Simple and effective resources were made available to households, businesses, and schools across the country to mitigate the impact of the outbreak. This effort could serve as a model for stemming much of the comparatively unsophisticated activity seen online, freeing up limited resources to focus on more advanced and persistent threats that impact both the public and private sectors.

- **Support greater public-private collaboration:** Businesses are heavily focused on guarding their operations from interruption and intrusion, preventing the loss of capital and intellectual property, and protecting public safety. They devote considerable resources to maintaining their operations in the wake of a natural hazard or man-made threat, such as a cyber attack. Industry expects that House legislation would serve to complement, not harm, the public-private partnerships existing under the National Infrastructure Protection Plan framework.

The business community recognizes the tremendous opportunities and challenges inherent in our interconnected world. Cyberspace has transformed the global economy and connected people in new and exciting ways. Any cyber legislation that Congress considers must protect and promote, not stifle, innovation in order to increase cybersecurity and grow electronic commerce.

Cyber threats change so quickly that any legislation must also protect the ability of the private sector to be fast and agile in the detection, prevention, mitigation, and response to cyber events that can have national or global impact. Policymakers should not complicate or duplicate

existing security-related industry standards with government-specific standards and bureaucracies.

Most significant, the House has an opportunity to take a positive, nonregulatory step forward on cybersecurity—as regulations would divert businesses' focus from security to compliance—by removing legal roadblocks that prevent the private sector and government from sharing cyber threat information while protecting personal privacy. We look forward to working with you on this important legislation.

Sincerely,

American Bankers Association
American Chemistry Council
American Fuel & Petrochemical Manufacturers
American Gas Association
American Petroleum Institute
Association of American Railroads
Bay Area Council
The Business Roundtable
Business Software Alliance
Consumer Bankers Association
CTIA–The Wireless Association
Edison Electric Institute
The Financial Services Roundtable
Information Technology Industry Council
Internet Security Alliance
National Association of Manufacturers
National Cable & Telecommunications Association
National Defense Industrial Association
The Real Estate Roundtable
Silicon Valley Leadership Group
Software & Information Industry Association
TechAmerica
TechNet
Telecommunications Industry Association
United States Telecom Association
U.S. Chamber of Commerce

Cc: Members of the U.S. House of Representatives