U.S. CHAMBER OF COMMERCE

1615 H Street, NW
Washington, DC 20062-2000
www.uschamber.com

October 28, 2014

Via www.sec.gov/cgi-bin/ruling-comments

Mary Jo White
Chair, Offices of the Commissioners
U.S. Securities and Exchange Commission
100 F Street, NE, Room 10700
Washington, DC 20549

Subject: Cybersecurity Roundtable, File No. 4-673

Dear Chairman White:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system, appreciates the Securities and Exchange Commission's (SEC's) discussion of cybersecurity issues at the commission's roundtable this past spring.[1] The Chamber understands that the SEC has established an internal cybersecurity working group, recommended by commission members.[2] We would welcome engaging the working group in a thoughtful dialogue on the cyber priorities of both organizations.

October 2014 marks the 11th Annual National Cyber Security Awareness Month. The cybersecurity of the American business community is a top Chamber priority. The need to address increasingly sophisticated threats against American and global enterprises has shifted from an information technology issue to a top concern of corporate boards and senior executives. In an interconnected world, economic security and national security are linked. To maintain a strong and resilient economy, industry and government must protect against the threat of cyberattacks.

[1] www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

[2] http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/sec-establishes-internal-cybersecurity-working-group/menu-id-1075.html?s=dn.

The Chamber supports the use of effective, relevant, and transparent disclosures to promote efficient capital markets. In the area of cyberattacks, the SEC must strike a balance between disclosures and other measures necessary to protect businesses and their investors. This balance and flexibility are necessary to ensure that the SEC is meeting its statutory mandate to protect investors while promoting competition and capital formation.

Information Sharing: More Constructive Than Compelled Disclosure

The Chamber is aware that some policymakers are pressing the SEC to leverage securities law and policy to compel businesses to report cyber risk and incident data with increasing specificity, including disclosing certain policy and technical controls and third-party security evaluations, which is troubling to many in industry.[3]

The Chamber favors constructive approaches to cybersecurity that reward creativity, speed, and innovation. Businesses need relatively minimal structure—such as the *Framework for Improving Critical Infrastructure Cybersecurity* (the framework)—and maximum autonomy to counter, in partnership with government, rapidly changing cyber threats. The business community takes cyber threats incredibly seriously, and the Chamber has witnessed significant support for risk-management tools like the framework.

Instead of forcing companies to disclose cyber incidents, the Chamber believes that passing information-sharing legislation with safeguards for businesses needs urgent attention by lawmakers and the administration. *We are advocating for businesses to disclose cyber incidents and threat data through a protected information-sharing program*. Further, the Chamber wants to expand government-to-business information sharing, which is progressing but needs improvement.[4] Companies tell us that they need more actionable and immediate threat data that only government entities have.

The Chamber seeks to incent companies to share cyber threat data with appropriate industry peers and civilian government entities to bolster our critical infrastructure, lifeline, first responder, and business systems.

The need for increased and actionable information sharing was raised repeatedly by roundtable participants. For example, Larry Zelvin, the former director of the U.S. Department of Homeland Security's (DHS') National Cybersecurity and Communications Integration Center, said that industry and government cannot have information security without greater information sharing, combined with legal clarity about what threat data companies can share with their peers and government.[5]

What is notable, federal securities law and policy already require registrants to disclose material cyber risks and incidents. Indeed, compelled disclosure that is injurious to a business may not

[3] www.sec.gov/comments/4-673/4673-11.pdf; see p. 7.

[4] www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-119_Jul14.pdf.

[5] www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt.

pass judicial muster.[6] The Chamber is concerned about efforts to expand the commission's role in deciding what a public company must report. Corporate boards are increasingly putting cybersecurity on their agendas, viewing cyber risk and threats as strategic and enterprise risk management priorities.[7]

Adding regulations would disrupt or damage trusted relationships between business and government needed to counter advanced and persistent attacks, which tend to originate overseas. Chamber members have constructive partnerships with federal agencies and departments—including Defense, DHS (the Secret Service), Energy, the FBI, and Treasury—to help companies manage cybersecurity incidents. We do not want these partnerships harmed because of new SEC reporting rules. Similarly, companies that contract with the government would face confusion when deciding how and when to report cyber information given the multiple and often conflicting guidance and rules.[8]

Above all, the Chamber believes that going beyond the SEC's 2011 guidance on cybersecurity[9] could paint a target on registrants' backs—including industry peers and supply chain partners—for no appreciable benefit to investors. Moreover, it is not clear that investors have asked for more disclosure from businesses regarding cybersecurity.[10] It is constructive that the SEC guidance recognizes that highly detailed disclosures could compromise a company's cybersecurity efforts by providing a road map for malicious actors that would seek to infiltrate a registrant's information networks. The commission appreciates that disclosures of this nature are not required under federal securities law.

Recommended Actions: Heighten Public Awareness, Pass an Information-Sharing Bill, Harmonize Cyber Rules, and Strengthen Deterrence

Cybersecurity is a significant Chamber priority. We are promoting the new framework, which was developed by the National Institute of Standards and Technology (NIST) in collaboration with the Chamber's Cybersecurity Working Group and other organizations, to help businesses of all sizes improve their security and resilience against cyber threats. Central to this effort is growing market-based solutions—products and services that Chamber members have created—for blocking and tackling malicious actors.

This year, the Chamber launched its national roundtable series, *Improving Today. Protecting Tomorrow*™, recommending that businesses of all sizes and sectors adopt fundamental Internet security practices. We organized roundtable events with state and local chambers in Chicago

[6] See *National Association of Manufacturers, U.S. Chamber of Commerce, and the Business Roundtable v. Securities and Exchange Commission*, 748 F.3d 359 (D.C. Cir. 2014).

[7] www.sec.gov/comments/4-673/4673-3.pdf; www.nacdonline.org/Cyber.

[8] www.nextgov.com/cybersecurity/cybersecurity-report/2011/10/sec-guidelines-good-intentions-fall-short/54930.

[9] www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[10] See June 6, 2011, letter to the Senate from the SEC, which states that investors are not asking for more disclosure in the area of cybersecurity.

(May 22); Austin, Texas (July 10); Everett, Washington (September 23); and Phoenix (October 8) prior to the Chamber's Third Annual Cybersecurity Summit on October 28.

But, policymakers need do much more, such as heightening public awareness of cybersecurity, passing cyber information-sharing legislation, harmonizing cyber regulations, and building a credible deterrence strategy to reduce cyber attacks.

- **Heightening public awareness of cybersecurity.** The Chamber urges policymakers to commit greater resources over the next several years to growing awareness of the framework and risk-based solutions through a national education campaign. A broad-based campaign involving federal, state, and local governments and multiple sectors of the U.S. economy would spur greater awareness of cyber threats and aggregate demand for market-driven cyber solutions.

  The Chamber believes that government—particularly independent agencies—should devote their limited time and resources to assisting resource-strapped enterprises, not trying to flex their existing regulatory authority. After all, while businesses are working to detect, prevent, and mitigate cyberattacks originating from sophisticated criminal syndicates or foreign powers, they shouldn't have to worry about regulatory or legal sanctions.

  The Chamber urges policymakers to commit greater resources over the next several years to growing awareness of the cyber framework and risk-based solutions through a national education campaign. A broad-based campaign involving federal, state, and local governments and multiple sectors of the U.S. economy would spur greater awareness of cyber threats and SEC disclosure laws and reporting requirements.

- **Passing information-sharing legislation.** Businesses want to participate in the online equivalent of a Neighborhood Watch program. Companies' security professionals seek to exchange cyber threat information and vulnerabilities with their peers and government, but they fear being penalized for doing the right thing. The Chamber strongly urges Congress to pass an information-sharing bill that contains strong protections related to lawsuits, public disclosure, regulations, and antitrust concerns and respects privacy.

  Indeed, the Chamber strongly support S. 2588, the Cybersecurity Information Sharing Act of 2014 (CISA), which the Senate Select Committee on Intelligence passed on July 8 by a strong bipartisan vote. This bill would promote business security and resilience against cyberattacks. It would be incredibly unfortunate if lawmakers finish the 113th Congress without passing CISA.

- **Harmonizing cybersecurity regulations.** Information-security requirements should not be cumulative. The Chamber believes it is valuable that agencies and departments are urged under the cybersecurity executive order to report to the Office of Management and Budget any critical infrastructure subject to "ineffective, conflicting, or excessively burdensome cybersecurity requirements." We urge the administration and Congress to prioritize eliminating burdensome regulations on businesses. One solution could entail giving businesses credit for information security regimes that exist in their respective sectors that they have adopted. It is positive that Michael Daniel, the administration's lead cyber official, has made harmonizing existing cyber regulations with the framework a priority.

The business community already complies with multiple information security rules. The SEC issued guidance in October 2011 outlining how and when companies should report hacking incidents and cybersecurity risks. Other regulatory requirements affecting businesses of all sizes include the Chemical Facilities Anti-Terrorism Standards (CFATS), the Federal Energy Regulatory Commission-North American Reliability Corporation Critical Information Protection (FERC-NERC CIP) standards, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley (SOX) Act. Corporations also comply with many non-U.S. requirements, which add to the regulatory mix.

- **Raising adversaries' costs through deterrence**. Policymakers who are pushing the SEC for greater disclosure of cyber attacks against businesses are putting the cart before the horse. Businesses are the victims of ongoing and serious cyber intrusions, launched by criminal gangs and foreign powers or their proxies. However, the U.S. government lacks a workable deterrence strategy—pushback that is timely and credible enough to better defend against the actions of bad actors.

  The Chamber is reviewing actions that businesses and government can take to deter nefarious actors that threaten to empty bank accounts, steal trade secrets, or damage vital infrastructures. While we have not formally endorsed the report, the U.S. Department of State's International Security Advisory Board (ISAB) issued in July draft recommendations regarding cooperation and deterrence in cyberspace.

  The ISAB's recommendations—including cooperating on crime as a first step, exploring global consensus on the rules of the road, enhancing governments' situational awareness through information sharing, combating IP theft, expanding education and capacity building, promoting attribution and prosecution, and leading by example—are sensible and worthy of further review by cybersecurity stakeholders.[11]

The Chamber believes that the United States needs to coherently shift the costs associated with cyber attacks in ways that are legal, swift, and proportionate relative to the risks and threats. Policymakers need to help the law enforcement community, which is a key asset to the business community but numerically overmatched compared with illicit hackers.[12] Deterrence is not only a cost issue but also a fairness issue. Beating back cyber attacks requires government and business working together, not bureaucratic government mandates.

[11] The ISAB report is available at www.state.gov/documents/organization/229235.pdf.

[12] The Chamber argues for a clear cyber deterrence strategy in its December 13, 2013, and October 10, 2014, letters to NIST on the framework. See http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html and http://csrc.nist.gov/cyberframework/rfi_comments_10_2014.html.

Let's Enhance Collaboration and Eliminate Barriers to Smart and Efficient Cybersecurity
The Chamber appreciates the opportunity to provide feedback to the cybersecurity roundtable. We are committed to protecting America's business community and enhancing the nation's resilience against an array of physical and cyber threats. Government and business entities need to continue leveraging smart and flexible risk-management tools like the cyber framework to strengthen collective security and make ongoing improvements.

Threats against businesses are increasing in sophistication and intensity. Instead of compelling businesses to publicly disclose information that could negatively affect them, companies seek the enactment of information-sharing legislation to achieve timely and actionable situational awareness to improve our detection, mitigation, and response capabilities. Businesses can learn from one another through timely sharing and help government officials build a panorama of threats facing the United States.

***

The Chamber welcomes the opportunity to offer our perspectives on cybersecurity policy. For further information, please do not hesitate to contact Ann Beauchesne [redacted]); Tom Quaadman [redacted], [redacted]); or our colleague Matthew Eggers ([redacted]).

Sincerely,

Ann Beauchesne

Ann M. Beauchesne
Vice President
National Security & Emergency Preparedness

Tom Quaadman
Vice President
Center for Capital Markets Competitiveness