Memorandum

January 28, 2013

To: Senator Rockefeller, Chairman of the Committee on Commerce, Science, and Transportation

From: Majority Staff, Senate Committee on Commerce, Science, and Transportation

Re: Summary of the Feedback on Cybersecurity from "Fortune 500" Companies

---

On September 19, 2012, you sent letters to the Chief Executive Officers of the five hundred largest companies in the United States, commonly referred to as the "Fortune 500." You wrote to the Fortune 500 to request information related to each company's views on cybersecurity and the *Cybersecurity Act of 2012*, the legislation that you, Senators Lieberman, Collins, Feinstein, Carper and others worked to pass during the 112th Congress. The letters asked the companies to describe the general process by which they developed their cybersecurity practices, the federal government's role in developing those practices, and the companies' concerns, if any, with specific provisions of the *Cybersecurity Act of 2012*. This memorandum provides an analysis of the responses to your letters.

As described in greater detail below, approximately three hundred companies in the Fortune 500 have now responded to your letters. The vast majority of the responses were thoughtful, thorough, and constructive. Overall, the companies' responses showed that the private sector is supportive of Congress's interest in passing cybersecurity legislation. Many companies stated that they supported the aims of the legislation, especially the provisions related to increased "information sharing" between the private sector and the federal government. Further, in contrast to the Chamber of Commerce's characterization of the legislation as creating an "adversarial relationship" between the federal government and the private sector, many companies recognized the importance of increased collaboration between the private sector and the federal government and, consequently, supported the aims of a voluntary federal program for the development of cybersecurity best practices, as envisioned in the legislation.

The concerns raised about the legislation were not about whether the government should have a role with respect to cybersecurity, but about the specifics of that role and what impact that role would have on how companies respond to their cybersecurity challenges. Many companies supported an increased government role and many supported the voluntary federal program envisioned in the *Cybersecurity Act of 2012*. However, many companies also raised concerns about any new federal program that would set mandatory cybersecurity requirements, create obligations that would impact their ability to address cybersecurity issues in a flexible manner, or duplicate efforts already underway. Although the current version of your legislation set no mandatory requirements, many companies were nevertheless wary of such an approach.

I. Background

On August 2, 2012, a filibuster blocked action on S. 3414, the *Cybersecurity Act of 2012*, with 52 Senators voting to act and 46 Senators supporting the filibuster. As you noted in your September 19, 2012, letter, the bill was blocked "largely due to opposition from a handful of business lobbying groups and trade associations, most notably the Chamber of Commerce." Leading up to the vote, the Chamber of Commerce had been very vocal in its opposition to the legislation and heavily lobbied against the bill. This opposition culminated in a letter it sent to every member of the United States Senate on July 31, 2012. In the letter, the Chamber attacked the substance of the bill and the process used to move the bill through the Senate.

The Chamber alleged that the bill had been "rushed to the floor without a legislative hearing or markup," even though the bill was based on two pieces of legislation that had each passed the Senate Commerce Committee and the Senate Homeland Security Committee, respectively, and had been the subject of numerous hearings and hundreds of meetings over a three and a half year period. The Chamber also argued that the legislation could "actually impede U.S. cybersecurity by shifting businesses' resources away from implementing robust and effective security measures and toward meeting government mandates," even though the bill had been amended to a purely voluntary approach. The Chamber stated:

> The regulatory approach provided in S. 3414 would likely create an adversarial relationship, which should be unacceptable to lawmakers. The Chamber urges Congress to not complicate or duplicate existing industry-driven security standards with government mandates and bureaucracies, even if they are couched in language that would mischaracterize these standards as "voluntary."

The Chamber ended its letter by stating it **"strongly opposes"** the *Cybersecurity Act of 2012* and that it could consider votes on the bill in its "annual *How They Voted* scorecard." Prior to this letter from the Chamber, on July 26, 2012, the Senate had voted 84 to 11 to proceed to the bill.

Following the filibuster, you sent letters to the largest companies in America to ask them a series of questions about cybersecurity and the legislation, to gauge whether the private sector was as opposed to your cybersecurity legislation as the Chamber of Commerce claimed it was. As cybersecurity will inevitably be a critical, ongoing issue that both the federal government and the private sector are forced to face, the letters were intended to: (1) raise awareness of cybersecurity as a national priority; and (2) elicit responses from companies to better understand the views of the private sector.

The following questions were included in the letter you sent to the Fortune 500 companies on September 19, 2012:

1. Has your company adopted a set of best practices to address its own cybersecurity needs?

2. If so, how were these cybersecurity practices developed?

3. Were they developed by the company solely, or were they developed outside the company? If developed outside the company, please list the institution, association, or entity that developed them.

4. When were these cybersecurity practices developed? How frequently have they been updated? Does your company's board of directors or audit committee keep abreast of developments regarding the development and implementation of these practices?

5. Has the federal government played any role, whether advisory or otherwise, in the development of these cybersecurity practices?

6. What are your concerns, if any, with a voluntary program that enables the federal government and the private sector to develop, in coordination, best cybersecurity practices for companies to adopt as they so choose, as outlined in the Cybersecurity Act of 2012?

7. What are your concerns, if any, with the federal government conducting risk assessments, in coordination with the private sector, to best understand where our nation's cyber vulnerabilities are, as outlined in the Cybersecurity Act of 2012?

8. What are your concerns, if any, with the federal government determining, in coordination with the private sector, the country's most critical cyber infrastructure, as outlined in the Cybersecurity Act of 2012?

II. Responses

To date, approximately three hundred companies in the Fortune 500 have now responded to your letters, with a response rate of over eighty percent for the largest one hundred companies.[1] The rate of response decreased as the size of the company decreased. While response rates dropped among smaller members of the Fortune 500, we view the overall response rate as a very positive sign that America's largest companies and top business executives are taking the issue of cybersecurity seriously. The vast majority of the responses were thoughtful, thorough, and constructive.

Our review of the companies' answers to these questions shows that the Chamber of Commerce's vehement opposition to the legislation was not shared by many companies in the private sector. Many companies provided support for provisions in the legislation and, when they raised concerns, they were offered in a thoughtful, constructive manner.

A. Cybersecurity Practices and the Federal Government's Role

The companies that responded all stated that they have developed cybersecurity practices to protect their infrastructure from cyber attacks. The practices were often based on compliance

[1] We anticipate that additional companies will provide responses, but believe enough have responded at this time to provide a summary. We will update this memorandum, if needed, as additional responses are provided.

with existing laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Energy Policy Act of 2005, the Sarbanes-Oxley Act of 2002, and the Financial Services Modernization Act of 1999 (commonly known as "Gramm-Leach-Bliley"). Many companies also noted their reliance on third-party audit firms to benchmark their cybersecurity practices and sector-focused trade groups, which have helped their development of practices.

Federal involvement in the development of private sector cybersecurity practices, outside of the aforementioned laws, varies by industry, but many companies cited the important role the National Institute of Standards and Technology (NIST) played in the development of their practices. NIST plays a role through its publication of cybersecurity standards and guidelines and companies stated that they relied upon NIST's expertise in developing their own practices.

Companies within the same industries also typically mentioned their involvement in government programs designed by sector-specific agencies with federal regulatory jurisdiction over their industries. For example, chemical companies cited their work with the Department of Homeland Security through the Chemical Facility Anti-Terrorism Standards (CFATS), financial companies discussed their work with the Department of the Treasury and the Federal Financial Institutions Examination Council, energy companies discussed the role of the Federal Energy Regulatory Commission, and communications companies highlighted their work with the Communications Security, Reliability, and Interoperability Council (CSRIC) developed by the Federal Communications Commission.

Companies' responses also acknowledged existing "information sharing" arrangements, including the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), the Federal Bureau of Investigation's InfraGard program, and the Department of Defense's Defense Industrial Base Voluntary Cyber Security/Information Assurance program ("DIB Pilot").

The companies' responses illustrated the federal government's current "ad hoc" approach for addressing the country's cybersecurity vulnerabilities and lend support to your view that better federal coordination, while respecting existing regulatory relationships, will help to improve and streamline the overall federal-private sector cybersecurity partnership. Your concern over the government's "ad hoc" approach was also shared by companies that provided responses. For example, one company stated the following in its explanation for why it supports a voluntary federal program:

> Vast federal resources are devoted to cybersecurity, but the current efforts are fragmented. We recommend the establishment of a public-private collaborative effort on cybersecurity that will combine existing federal requirements under a single coordinated framework. This approach will minimize undue complexity and promote a more agile and effective national cybersecurity response.

B. Positions on the Legislation

Very few companies stated in their responses that they were in outright opposition to the *Cybersecurity Act of 2012* and only a subset of those explicitly characterized their positions as "in line with those of the Chamber of Commerce." Most companies supported Congress's

efforts to pass cybersecurity legislation and provided thoughtful responses that included their critique of specific provisions of your bill. Many companies supported your proposal to create a voluntary federal cybersecurity program, where the federal government and the private sector work together to address the country's cyber vulnerabilities. Example responses from companies are provided below.[2]

Title I, Public-Private Partnership to Protect Critical Infrastructure Many companies supported a voluntary program to protect critical infrastructure, so long as it would not become mandatory. These statements included the following.

- A global financial company stated, "We support a voluntary program that enables the federal government and the private sector, in coordination, to develop best practices for companies to adopt as they so choose."

- A global conglomerate stated, "We welcome the opportunity to partner with the federal government to help identify our country's cyber vulnerabilities, and jointly develop protective measures that will promote the safeguarding of information critical to national security."

- A national retail chain stated, "We agree that collaborative efforts between government and business are essential in undertaking the significant challenges related to cybersecurity, much like partnerships we currently have for disaster response and recovery."

- A healthcare company stated, "We recommend the establishment of a public-private collaborative effort on cybersecurity that will combine existing federal requirements under a single coordinated framework."

- A technology company stated it "supports the development of cybersecurity best practices for voluntary adoption and use at critical assets" and "supports a critical infrastructure identification process jointly operated by the public and private sector, based on risk."

Many companies were in favor of a voluntary program to develop cybersecurity best practices, and many companies supported using the program to conduct risk assessments and to identify the nation's most critical infrastructure.

Companies' concerns related to the proposed voluntary program were primarily related to the potential development of an inflexible, "one-size-fits-all" set of best practices, and companies in the financial and electric sectors in particular expressed concern that their existing regulatory relations would be disrupted. Other common concerns included the need to adequately protect the confidentiality of information shared with the federal government during cyber threat assessments, and whether existing critical infrastructure programs, such as DHS's National Infrastructure Protection Plan, would be needlessly duplicated.

[2] Additional examples of company statements about the legislation are provided in the attached table.

In addition to the companies that provided supportive statements or their specific concerns, some companies did explicitly state they were in outright opposition to Title I. For example, one company wrote it "did not support the Cybersecurity Act of 2012 when it was being considered by the Senate this summer" because it believed the legislation would lead "to [a] kind of top-down, 'check-the-box' compliance regime."

Title VII, Information Sharing. Although your letter did not specifically ask for companies' views on "information sharing," many companies proactively stated that they supported increased information sharing between the federal government and the private sector through legislation.

- An oil company stated, "We greatly value the government's role in collecting and analyzing information about cybersecurity threats, and believe that sharing this information with private industry strengthens all our efforts."

- A healthcare company stated, "We recommend that the government accelerate our nation's cybersecurity preparedness through the promotion of public-private partnerships that will facilitate exchange of strategic threat assessments and other pertinent intelligence . . . This will enable private sector entities that own or operate major information systems and other critical infrastructure systems to respond to emerging cybersecurity threats on a timely basis."

- An energy company stated, "We greatly value the government's role in providing current data about cybersecurity threats . . . We believe that this approach is well suited to the needs of private industry, and results in swift and effective cybersecurity measures."

Nearly every company that provided a thorough response expressed support for more robust, two-way cyber threat information sharing, with greater access to security clearances to ease the process.

Other Provisions. While the letter did not explicitly ask for views on other provisions of the *Cybersecurity Act of 2012*, a number of companies supported the legislation's research and development, public awareness, and workforce provisions. Support for greater cybersecurity research and development and workforce training, in particular, was noted by a variety of companies, including energy companies and manufacturing companies.

III. Conclusion

The responses showed that you should continue working to advance cybersecurity legislation in the 113th Congress. Many companies were generally supportive of your efforts and many of their concerns could be addressed through a revised bill introduced this year. Many companies expressed support for a federal program that enables the private sector and the federal government to voluntarily work together to determine the greatest cyber risks facing the country and the best path forward to address them. The concerns with such a program were generally related to the manner in which it would be implemented, not with the fundamental notion of whether to create it. American companies recognize the importance of securing our most critical infrastructure from cyber attack and recognize the need for a government role.