



---

U.S. CHAMBER OF COMMERCE

---

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

November 7, 2016

Mr. Donald S. Clark  
Secretary  
Federal Trade Commission  
600 Pennsylvania Avenue, N.W.  
Suite CC-5610 (Annex B)  
Washington, DC 20580

**Re: Safeguards Rule, 16 C.F.R. 314, Project No. P145407.**

Dear Mr. Clark:

The U.S. Chamber of Commerce (the “Chamber”) is the world’s largest business federation, representing the interests of more than three million companies of every size, sector, and region. Strong and appropriate policies promoting cybersecurity and consumer protections are an important and necessary component of efficient capital markets.

We are grateful for the opportunities we have had to partner with the Federal Trade Commission (“Commission”) on the cybersecurity challenges facing American businesses. The Chamber appreciates the opportunity to respond to the request for public comment of the Commission regarding its Standards for Safeguarding Customer Information (the “Safeguards Rule”).<sup>1</sup> The Commission has played an important role in the cybersecurity and data privacy fields, and it will have a substantial part to play in determining whether businesses and the government can collaborate effectively going forward—or whether that relationship will be an adversarial one. To that end, we would ask the Commission to adopt policies that encourage businesses to continue investing in cybersecurity.

We consequently write to emphasize three points:

---

<sup>1</sup> See *Standards for Safeguarding Customer Information*, 81 Fed. Reg. 61632 (Sept. 7, 2016) (“Comment Request”).

- **A broad consensus has emerged that the private sector and the public sector must collaborate on cybersecurity challenges.**
- **The Commission should not expand the Safeguards Rule in a manner that deters collaboration between the private and public sectors.**
- **The Commission should focus on enhancing its collaboration with industry, including by harmonizing and streamlining regulations.**

We believe that collaboration between industry and government is critical to addressing those challenges effectively. As an independent regulatory agency with enforcement authority in this area, the Commission must be careful not to deter or undermine this collaboration going forward. The Commission has taken important steps in this direction to date, including by emphasizing its education and outreach function, through publications such as *Start With Security* (2015) and related public events, and its recent explanation of how its work tracks to the National Institute of Standards and Technology Framework for Critical Infrastructure Cybersecurity v. 1.0 (the “NIST Framework”).<sup>2</sup> We hope that the Commission will continue to build a collaborative relationship with industry rather than expand the Safeguards Rule and its resulting compliance burden.

**(1) A Broad Consensus Has Emerged That The Private Sector And The Public Sector Must Collaborate On Cybersecurity Challenges.**

Private-sector businesses own and operate the substantial majority of the critical infrastructure in the United States, including in the financial services industry. While the government has an important role to play in supporting private sector cybersecurity, U.S. businesses ultimately are responsible for protecting their networks, systems, and data. This includes not only preventing trade secret theft and system manipulation, but also stopping the compromise of the personal information of their employees and customers. Businesses accordingly have made enormous investments

---

<sup>2</sup> Andrea Arias, FTC, *The NIST Cybersecurity Framework and the FTC*, FTC: Business Blog (Aug. 31, 2016), <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc>.

into a wide range of cybersecurity tools and have organized themselves to ensure that these tools and related internal policies function as effectively as possible.

Against this backdrop, it has become a truism that the government and the private sector must work together—not at cross purposes—to enhance our nation’s cybersecurity. The Obama administration and Congress both have built their cybersecurity policies around this basic premise. Three particular policies merit special focus:

*First*, the NIST Framework—which was released in February 2014—has been a notable success and a clear marker of the benefits of public-private collaboration on cybersecurity challenges.<sup>3</sup> The Chamber, sector-based coordinating councils and associations, companies, and other entities have collaborated closely with NIST in creating the framework from the first workshop in April 2013 to its ongoing implementation. Critical infrastructure entities are very supportive of the NIST Framework. Indeed, businesses across the U.S. economy have incorporated the NIST Framework or similar risk management tools into their cybersecurity programs. This is because NIST has created a broadly-applicable platform for long-term strengthening of cyber defenses, rather than static checklists that will be quickly outdated.

*Second*, the government and private sector agree that the timely sharing of actionable cyber threat data offers an important first line of defense against cyber threats. Following a bipartisan push in the House of Representatives and the Senate last year, President Obama signed the Cybersecurity Information Sharing Act into law. This landmark legislation gives businesses the legal protection they need to feel safe when voluntarily sharing or receiving threat data with industry peers and the government. The Chamber now is working with government to turn this shared goal of effective, real-time information sharing into a reality, working with the government to encourage collaborative—and thus effective—cybersecurity.

*Third*, President Obama recently provided additional clarity on how the federal government will participate in the response to cybersecurity incidents in the private

---

<sup>3</sup> See NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Feb. 12, 2014). See also Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013).

Mr. Donald S. Clark  
November 7, 2016  
Page 4

sector by issuing a Presidential Policy Directive on cyber incident coordination.<sup>4</sup> As Michael Daniel, special assistant to the president and White House cybersecurity coordinator, said at a U.S. Chamber roundtable on the topic, the directive “brings together the lessons learned from responding to cyber events over the last eight years,” and provides additional clarity and guidance to the private sector “about the federal government’s roles and responsibilities” in responding to incidents that affect the private sector.<sup>5</sup> As a result, companies now have more clarity about what they can expect from the government, allowing the development of more effective working relationships.

Likewise, the Commission has taken steps towards a more collaborative approach to enhancing private-sector cybersecurity. It has emphasized its education and outreach functions, including by describing what it views to be key elements of effective cybersecurity programs in its *Start With Security* publication in 2015 and related engagement with industry stakeholders. The Commission also recently published a blog post in which it explained that its view of effective cybersecurity risk management is consistent with the NIST Framework.<sup>6</sup> Both steps have given the welcome signal that the Commission wants to help companies, not merely second guess them after they have been attacked by cyber criminals or other threat actors.

But more remains to be done. As Commerce Department Secretary Penny Pritzker recently said at the Chamber’s Cybersecurity Forum, “we still need more strategic, real-world cooperation between government and industry.”<sup>7</sup> To accomplish this goal, we need to continue to close the trust gap between the private sector and government. The private sector must have comfort that working with government will not lead to regulatory second-guessing that deters companies from coming forward in the future. To achieve this goal, the government must continue to strengthen its relationships with industry: as Secretary Pritzker explained, the federal government “must change the value proposition for businesses to engage with

---

<sup>4</sup> Presidential Policy Directive/PPD-41, United States Cyber Incident Coordination (July 26, 2016).

<sup>5</sup> Ann M. Beauchesne, *Government, Business Staying in Step to Put Out Cyber Fires*, U.S. Chamber, of Commerce: Above the Fold (Aug. 8, 2016).

<sup>6</sup> See Arias, *supra* n. 2.

<sup>7</sup> U.S. Secretary of Commerce Penny Pritzker, Address to U.S. Chamber of Commerce’s Cybersecurity Summit (Sept. 27, 2016).

government—before, during, and after cyberattacks.”<sup>8</sup> The Commission has an important role to play in achieving this goal.

**(2) The Commission Should Not Expand The Safeguards Rule In A Manner That Deters Collaboration Between The Private And Public Sectors.**

In contrast to the consensus around the need for a collaborative, risk-based approach to cybersecurity, most observers agree that we cannot regulate our way out of cyber threats. Regulations cannot possibly keep pace with cyber threats. Their expansion would lead to check-the-box security mandates that are costly, time-consuming, and ineffective—thus pulling businesses’ limited resources away from cybersecurity and toward compliance. This development would harm the very collaboration that experts agree is critical to addressing our nation’s cybersecurity challenges. As Secretary Pritzker put it, “[t]he problem is that relationships between regulators and the businesses they regulate are inherently adversarial—NOT collaborative.”<sup>9</sup>

We urge the Commission to avoid taking any step that would make the relationship between government and the private sector more adversarial on cybersecurity matters. Specifically, the Commission should not expand the Safeguards Rule in a manner that creates new requirements for regulated entities or expands the number of regulated entities subject to the rule.

We do not expect the Commission to limit the existing scope of the Safeguards Rule at this time. But expanding the scope of the rule—whether in terms of the requirements it imposes or the entities it covers—would send the wrong message to industry stakeholders at a time when the public and private sectors are working hard to build collaborative relationships. This is particularly true given that the Commission’s existing statutory authorities give it the tools it needs to play a leading role in privacy and cybersecurity matters. Expanding the Safeguards Rule in this manner thus is unnecessary to achieve the Commission’s mission—and would needlessly impose additional compliance burdens on companies. In doing so, the Commission would divert more company resources from enhancing security to

---

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

documenting compliance, and shift companies' focus from responding to rapidly evolving threats to ensuring satisfaction of static checklists. In short, the Commission would tangle information security teams up in yet more red tape, rather than empower them to tackle the cybersecurity challenges their companies face.

Moreover, it is no answer to say that an expanded Safeguards Rule would be built around the NIST Framework. Using the NIST Framework as a regulatory tool is bound to drive companies from the framework process, both with respect to its adoption and its further development. Such a loss of industry engagement in the NIST Framework process would be highly counterproductive and ultimately hurt consumers. The Chamber does not want this outcome, and the Commission should not want it either. Moreover, the NIST Framework is, by its nature, a flexible tool that enables companies to address the particular cybersecurity challenges they face. It encourages them to do so in a risk-based manner tailored to the design of the networks they operate, the nature of the systems they own, and the character of the data they hold. The Commission cannot use the NIST Framework as a regulatory tool without distorting it so that its use is no longer an exercise in cybersecurity risk management, but an exercise in regulatory risk management.

To be sure, the Chamber does not expect the Commission to get rid of “ineffective, conflicting, or excessively burdensome cybersecurity requirements” overnight.<sup>10</sup> But we do believe that the Commission, like other policymakers, should refrain from proliferating new red tape on cybersecurity, since doing so is contrary to effective risk-management.

**(3) The Commission Should Focus On Enhancing Its Collaboration With Industry, Including By Harmonizing And Streamlining Regulations.**

Rather than creating more regulatory requirements, the Commission should focus its efforts on building effective partnerships with industry. The Commission has extensive experience working on cybersecurity and privacy issues facing companies of all sizes and across a wide range of industries. The Commission should leverage that experience to help businesses develop workable solutions to the

---

<sup>10</sup> See Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, *supra* n. 3.

cybersecurity challenges that they face. Second-guessing companies after a compromise is easy; the Commission should focus on the hard work of helping companies prioritize their limited resources to address the numerous and evolving threats from criminals, hostile nation states, and other threat actors. In doing so, the Commission can help to close the trust gap between industry and government and to support the collaboration necessary to strengthen our nation's cybersecurity.

We would urge the Commission to take three particular steps:

*First*, the Commission should work to harmonize its regulatory approach with other regulatory agencies and streamline regulations to the maximum extent possible. Many companies already must comply with a number of federal and state regulatory requirements relating to cybersecurity. Despite numerous calls for regulatory harmonization, there has been no concerted effort to-date to identify and eliminate duplicative or contradictory regulations. As a result, companies face unnecessary compliance burdens that could be readily lightened by regulators simply coming together to identify workable solutions. As a regulator with wide-ranging authority, the Commission can play a particularly valuable role in these efforts. And by simplifying and clarifying the tangle of cybersecurity regulatory requirements that companies must satisfy, the Commission can empower companies to focus more on security and less on compliance, and thereby protect consumers more effectively from cyber threats. The Commission has sought to take on a leadership role on cybersecurity issues; reducing the energy wasted on duplicative and redundant cybersecurity compliance efforts would be worthy of that role.

*Second*, the Commission should work to encourage further voluntary adoption and refinement of the NIST Framework. As discussed, Version 1.0 of the NIST Framework has been the product of a very high degree of collaboration between the public sector and the private sector. Its long-term success will turn on whether industry and the government can work together to continue to develop and support the NIST Framework, and, ultimately, whether the private-sector can assume leadership of the NIST Framework going forward. The Commission should fully support these efforts. It previously has explained that its efforts are generally consistent with the approach taken in the NIST Framework.<sup>11</sup> It should do more now

---

<sup>11</sup> See, e.g., Arias, *supra* n. 2.

Mr. Donald S. Clark  
November 7, 2016  
Page 8

to support adoption of the NIST Framework by companies of all sizes and across all industries. By encouraging the broad-based adoption of a common approach to cyber risk-management, the Commission would make clear that it shares the vision of a collaborative approach to enhancing national cybersecurity.

*Third*, the Commission should expand its efforts to educate companies of all sizes about the tools and strategies they can use to most effectively secure their networks. Though often focused on regulatory or enforcement actions, the Commission is well-positioned to deliver valuable and timely insights to businesses that are struggling to protect their systems and data against the sophisticated threats they face, particularly given budget constraints. The Commission would be a valuable partner to those companies, so we urge it to take on that role more vigorously going forward.

\* \* \* \* \*

American businesses—and by extension, the customers they serve—face substantial cyber threats. Companies have invested heavily in addressing these threats directly and in building collaborative relationships with government and industry stakeholders to ensure that security is strengthened broadly across the economy. The Commission should encourage those efforts and work to build trust between the government and the private sector. In contrast, expanding the Safeguards Rule would send the wrong message to industry, deterring collaboration and causing companies to focus on regulatory compliance rather than on security. We consequently urge the Commission to refrain from expanding the Safeguards Rule at this time.

We thank you for your consideration of these comments and would be happy to discuss these issues further with appropriate staff.

Sincerely

Tom Quaadman  
Executive Vice President  
Center for Capital Markets  
Competitiveness

Ann Beauchesne  
Senior Vice President  
National Security and  
Emergency Preparedness