U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness

1615 H Street, NW
Washington, DC 20062
202-463-3100

July 8, 2016

Via Joan.Rolf@nrc.gov

Joan Rolf
Senior Cyber Security Coordinator
Nuclear Regulatory Commission
Washington, DC 20555

Dear Ms. Rolf:

The U.S. Chamber of Commerce appreciated the opportunity to appear in April before the Cybersecurity Forum for Independent and Executive Branch Regulators (the Cyber Forum), which was hosted by the Federal Trade Commission (FTC) and the Federal Drug Administration (FDA), concerning self-regulatory approaches to cybersecurity.

During the gathering, public- and private-sector participants discussed (1) various third-party guidance, standards, and frameworks available to inform companies' cybersecurity programs; (2) the interplay between self-regulatory approaches to cybersecurity and the role of law enforcement; and (3) ways in which law enforcement entities and regulators can work together to improve the use of self-regulatory approaches across sectors.[1] For several years, the Chamber has been partnering with government toward smart and practical solutions connected to these and many other cybersecurity policies. Engaging the Cyber Forum advances this trend.

The Chamber provides the following points to explain how we view these three broad issues that the Cyber Forum asked participants to grapple with. This past spring, the Chamber walked through our February 9 letter to the National Institute of Standards and Technology (NIST) regarding the *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework), which speaks to topics No. 1 and No. 2. Still, we want to (1) provide the Chamber's perspectives in writing for the record; (2) highlight recent Chamber activities concerning a new information-sharing program and norms and deterrence policy; and (3) bring attention to the role of law enforcement, which is not dealt with extensively in our letter to NIST but is significant to bolstering U.S. cybersecurity.[2]

The joint industry-NIST Framework is a sound baseline for businesses' cybersecurity practices. A new agency rulemaking undercuts the bottom-up, collaborative approach to cybersecurity policy. A positive course correction is still possible.

The Chamber believes that most businesses and policymakers see the Framework as a key *pillar* for managing enterprise cybersecurity risks and threats, including at home and increasingly abroad.[3] NIST did an admirable job convening industry to develop the Framework over the course of many months. The Chamber will be pressing the next administration to embrace the Framework. We see the Framework as a multistakeholder tool, as a collaborative process, and as a constructive mind-set. The Chamber urges private organizations—from the C-suite to the newest hire—to commit to robust cybersecurity practices.

To sustain the momentum behind the Framework, the Chamber believes that both industry and government have jobs to do. On the one hand, the Chamber has been actively promoting the Framework since it was released in 2014. Our national cybersecurity campaign is funded through members' sponsorships and the financial and in-kind contributions of state and local chambers of commerce, other business organizations, and academic institutions. Further, Chamber members are using the Framework and urging business partners to manage cybersecurity risks to their data and devices. Industry is working with government entities, including the Department of Homeland Security (DHS), to strengthen its information networks and systems against a dizzying array of malicious actors.

On the other hand, the Chamber urges policymakers to help agencies and departments harmonize existing regulations with the Framework and maintain the Framework's voluntary nature. The Chamber said to the Cyber Forum in April that some government entities are forming genuine partnerships with industry to enhance the security and resilience of U.S. critical infrastructure; some agencies are seemingly exploring ways to flex their regulatory muscles; and some federal bodies are apparently abandoning the spirit, if not the precepts, of the 2013 cybersecurity executive order (EO) and the Cybersecurity Enhancement Act of 2014. Both measures call for modernizing cybersecurity rules.

A single business organization should not be beset by multiple cybersecurity rules coming from many agencies, which are likely to be conflicting or duplicative in execution. The Chamber holds that policymakers, including members of the Cyber Forum, should appoint an official(s) to focus on reducing duplicative, if not eliminating, overly burdensome cybersecurity requirements impacting regulated organizations, as called for under the 2013 EO and the 2014 act.

In addition to urging regulatory harmonization, our organization opposes the creation of new or quasi-cybersecurity regulations, especially when government authorities have not taken affected entities' perspectives into account. A case in point is the Federal Communication Commission's (FCC's) proposed broadband privacy rule. The Chamber believes that the FCC needs to dramatically pull back on this rulemaking. Above all, the FCC's rulemaking represents the opposite approach to shared, cooperative public-private cybersecurity that the Obama administration and the Chamber are holding up as a model for stakeholders to imitate.

The Chamber opposes the Commission's mandates for at least four reasons:

First, industry presented many of its concerns, which the Chamber shares, with the FCC's proposed regulations on June 14 before a congressional panel.[4] The Chamber also wrote to the

FCC on May 26 saying that the rule is unnecessary, exceeds statutory authority, and threatens innovation by stifling the already thriving internet. The Commission is rushing a top-down, complicated rulemaking that would benefit from lengthier, in-depth scrutiny. The Chamber said that the FCC should abandon its current regulatory approach under the proposed rulemaking and adopt a privacy architecture similar to that of the FTC's, which protects consumers effectively while enabling businesses to innovate.[5]

Second, the proposed broadband privacy rule undermines the bottom-up, collaborative approach to cybersecurity policy that the Chamber and many industry organizations are advancing with government partners domestically and overseas.[6] Further, the FCC's proposed rulemaking is overly privacy centric. There is a strong consensus among security professionals that effective approaches to cybersecurity should be risk management centric. And the Framework, per the cybersecurity EO, includes a methodology to protect individual privacy and civil liberties when organizations conduct cybersecurity activities.

Third, the Chamber supported the public-private Communications Security, Reliability and Interoperability Council (CSRIC) IV's adoption in March 2015 of the *Cybersecurity Risk Management and Best Practices (Working Group 4)* report. The communications sector—made up of the broadcast, cable, satellite, wireless, and wireline industries—spent a year developing its cybersecurity report. Producing this report consumed the time of approximately 100 cybersecurity professionals. Among other things, the working group developed guidance to help communications providers use the Framework to make the availability of the core network infrastructure more resilient and guard people's privacy. The Chamber applauded the CSRIC IV initiative because it showed real leadership on cybersecurity by both industry and government.

Fourth, what particularly frustrates the Chamber about the FCC's proposed rule is that we urge industry organizations to use the Framework and drive productive initiatives like CSRIC IV. However, the FCC is apparently backtracking on prior commitments to pursue a new regulatory model vis-à-vis the communications sector. In June 2014, FCC leadership challenged the communications sector to "create a 'new regulatory paradigm' of business-driven cybersecurity risk management"—and sector stakeholders stepped up in a major way.[7] The CSRIC IV endeavor both enhances the security of communications providers and protects individuals' privacy. But the Commission has seemingly turned its back on CSRIC IV in favor of "traditional regulation"—an approach that the FCC originally rejected.[8]

Big picture: The Chamber thinks that members of the Cyber Forum should care a great deal about industry's views concerning the FCC's unwarranted regulatory actions. Government and businesses have mutual interests in fostering quality public-private cybersecurity relationships. Neither the Chamber nor the Cyber Forum should want to send industry the message that pursuing public-private partnerships comparable to CSRIC IV are hollow gestures. The ink on the adaptive CSRIC IV initiative was barely dry before some authorities brushed it aside in favor of a compliance-based regime, which is ill-suited to respond effectively to today's complex cybersecurity environment. The Cyber Forum should understand that it's nearly impossible for the Chamber to promote public-private collaboration if only one party in the relationship is willing to make it work.

An objective of the Cyber Forum is to "align, leverage, and deconflict cross-sector regulatory authorities' approaches"[9] in the name of bolstering U.S. cybersecurity. The Cyber Forum should include the FCC's proposed rule in an upcoming meeting. The discussion could examine how the regulations may have counterproductive implications for national cybersecurity policy and activities. Positive outcomes are still possible. The Chamber was impressed with the open, problem-solving approach that the Cyber Forum took to its deliberations in April.

What's perhaps useful to the interagency forum is that industry actors occasionally leverage their influence to urge their business partners to make prudent course corrections on cybersecurity matters. The takeaway is that such actions are analogous to a mentoring program whose benefits accrue not only to the parties most affected but also to the system as a whole. Likewise, the Cyber Forum could evaluate the FCC's rules in an equally tough-minded yet considerate way.

The Framework is part of a mix of cybersecurity policy initiatives that need to move forward together.

It is important to stress to the Cyber Forum that the Framework is part of a collection of cybersecurity policies that need to advance together.

Here are some select issues that are worth highlighting for forum members:

The Cybersecurity Information Sharing Act of 2015

First, the Chamber testified on June 15 before a House Homeland Security Committee subcommittee on the Cybersecurity Act of 2015, including the Cybersecurity Information Sharing Act of 2015 (CISA), which is title I of the 2015 act.[10]

The Chamber's public message regarding CISA was threefold:

- The CISA program is off to a good start. Final CISA and Automated Indicator Sharing (AIS) implementation guidance documents were finalized on June 15. The Chamber is reviewing them with our members. We appreciate the open and constructive discussions that the Chamber had with DHS and Department of Justice (DOJ) officials, who authored the guidance. The Chamber said that while oversight by Congress is crucial, it is too soon to make changes to the legislation. CISA does not need to be reauthorized for several years (i.e., September 2025).

- We thank policymakers for getting the cybersecurity information-sharing legislation across the finish line. And we urge lawmakers and the administration to be industry's ally as they use the program. Companies need to feel that policymakers have their backs. It is important that businesses see that the protections granted by the law—including matters tied to limited liability, regulation, antitrust, and public disclosure—become real.

- We tell businesses that they should use the Framework, join an information-sharing and analysis organizations (ISAO) or an information-sharing and analysis center (ISAC), and take advantage of the CISA/AIS system as appropriate. The Chamber urges the senior

leaders of industry groups to promote these initiatives among their peers and constituencies.[11]

Cyber incident data and analysis repository

Second, the Chamber supports piloting a CIDAR—shorthand for a cyber incident data and analysis repository. In May, we sent a letter to DHS saying that (1) data submitted to a CIDAR need to be made anonymous, (2) additional sharing protections will probably be needed, and (3) an experimental CIDAR could offer tangible upsides to public- and private-sector cybersecurity. Comprehensive information about cyber events could assist insurers in expanding cyber coverage and in identifying cybersecurity best practices for their customers.

The idea behind the CIDAR is to provide a platform for enterprise owners and insurers to discreetly share, store, aggregate, and analyze sensitive cyber incident data. The CIDAR should specifically aid in expanding the "cyber" insurance market in healthy ways. The Chamber wants to help increase the sound buying of cybersecurity insurance beyond a few key sectors (e.g., banking and financial services, health care, retail, and technology) and large organizations, which are the principal purchasers of coverage today.

Wassenaar Agreement control language governing 'intrusion software' and surveillance items

Third, the Chamber appreciates the efforts of the administration to renegotiate the Wassenaar Agreement (WA) control language governing so-called intrusion software and surveillance items, which are aspects of a controversial international agreement to prevent the export of sophisticated hacking tools to repressive governments and criminal organizations. Industry and democratic governments have a shared interest in keeping malicious software out of the hands of bad actors. But the 2013 WA control language governing intrusion software and surveillance items takes a seriously wrong approach to cybersecurity.[12]

WA officials gathered from June 20 to 24 in Vienna, Austria, at the working group level. The Chamber is encouraged by reported progress during the Vienna talks, but there's much more work to be done.[13] Industry is urging officials to completely eliminate the controls on technology, software, and hardware. If deleting the controls is not possible, the Chamber and many others recommend that WA officials substantially narrow the scope of the control language and dramatically simplify the language in order to bring clarity and enable compliance.[14] If the WA control language is not eliminated or at least adequately amended, it could have a powerfully (unintended) negative effect on businesses' cybersecurity and on the CISA program in particular. Creating cybersecurity policies and laws in the WA environment lacks sufficient transparency and does not advance public-private partnerships at home and globally.

Cybersecurity norms and deterrence

Fourth, on June 8, the Chamber's board of directors approved a policy statement on cybersecurity norms and deterrence. The statement argues that despite the existence of written blueprints, such as ones related to global prosperity and defense, the U.S. cybersecurity strategy is seemingly uncertain—both to many in the private sector and our adversaries alike. The Chamber believes that policymakers need to refocus national and global efforts to heighten the costs on sophisticated attackers that would willfully hack America's private sector for illicit purposes.

Public-private policymaking needs to spotlight increasing adherence to international norms and deterrence to reduce the benefits of conducting harmful cyber activity against the U.S. business community and the nation. The statement makes several policy endorsements. For example, the Chamber contends that the United States and its allies should assist law enforcement entities in curtailing cybercrime. Authorities should also avoid blaming the victim, including placing disproportionate burdens for deterrence and liability on the private sector. Governments need to enhance their capacities to weaken nefarious organizations and individuals. Countries should not allow safe havens from which illicit hackers are able to attack U.S. interests.

Law enforcement wants to be an industry partner, not an extension of regulatory agencies. Policymakers need to devote more government capacity to thwarting cyberattacks.

The Chamber's overwhelming experience concerning law enforcement, including the FBI and the Secret Service, is that authorities do not want to be viewed as an extension of the regulatory community.

We believe that at least two factors drive law enforcement entities' desire to cooperate with industry:

First, on April 26, FBI Director James Comey urged businesses to inform the Bureau about cyber incidents and to work with the FBI and other government agencies to identify cyber threats. The Bureau is charged with investigating and building cases against bad actors—particularly individuals and groups that are operating overseas—and the FBI needs industry to share evidence of hacks and attempted hacks with it.

Director Comey said that the Bureau would not share the information with regulators, and he noted that fears of regulatory consequences are inhibiting some companies from participating in sharing cyber threat data. His views track with the concerns that we regularly hear from businesses. "We will not share your data" with anyone, Comey said, adding that companies should report to "avoid being victimized over and over again" by hackers.[15] The Chamber appreciates the director's attitude and thinks that it sends a constructive message to the private sector. To be sure, the FBI likely intends to share cyber threat signatures with other parties but withhold business-sensitive data.

Running a close second, the Chamber believes that companies hacked by foreign governments and amply resourced criminal groups often face unwarranted blame, including shouldering disproportionate burdens for deterrence and liability. Governments should reject a blame the victim mentality when it comes to cyber intrusions. The Chamber agrees with Assistant Attorney General for National Security John Carlin who says, "Blaming companies for sophisticated breaches by nation-states is akin to blaming a pedestrian who gets stabbed by a stranger for simply making eye contact beforehand."[16] Similarly, at a recent meeting with FBI officials, a special agent told Chamber members, "We [the FBI] put the victim first—this is a cultural change. We do not want to put handcuffs on the private sector."

Cybersecurity Forum for Independent and Executive Branch Regulators[17]	
Members	Law enforcement role comparable to the FBI and the Secret Service? (Y/N)
Nuclear Regulatory Commission (NRC), chair	N
Federal Communications Commission (FCC)	N
Federal Energy Regulatory Commission (FERC)	N
Securities and Exchange Commission (SEC)	N
Federal Trade Commission (FTC)	N
Federal Reserve Board (Fed)	N
Federal Financial Institutions Examination Council (FFIEC)	N
Financial and Banking Information Infrastructure Committee (FBIIC)	N
National Association of Insurance Commissioners (NAIC)	N
Other agencies or departments may participate as appropriate	TBD
National Institute of Standards and Technology (NIST), a nonregulatory body, serves as an adviser to the Cyber Forum	NA

The table is meant to illustrate the numeric mismatch between government entities, including members of the Cyber Forum, that are empowered to regulate the business community and government entities that are tasked with investigating and prosecuting cybercrimes. The Chamber supports increasing the resources that law enforcement agencies need to counter and mitigate cyber threats internationally. The Cyber Forum should consider how its members can help law enforcement increase costs on malicious actors. We need more private sector and government capacity beyond the FBI and the Secret Service—which are just 2 federal entities out of 15 executive branch departments and dozens of independent agencies—pushing back on malicious actors.[18]

Policymakers need to help the law enforcement community, which is a key asset of the business community but numerically overmatched compared with hackers. The DOJ's Carlin recently wrote an article in the *Harvard National Security Journal*, noting, "No one agency can beat the threat. Instead, success requires drawing upon each agency's unique expertise,

resources, and legal authorities, and using whichever tool or combination of tools will be most effective in disrupting a particular threat."[19]

The government has committed extensive sums to working with the private sector to battle cyberattacks against the business community. Yet government entities are arguably hesitant to confront the vast majority of the cyber hostilities that beset the private sector—or what the Chamber terms the "malicious middle" in our June 8 cyber norms and deterrence policy paper.[20] Meanwhile, businesses' cybersecurity budgets are increasing, which is positive. However, cyber defense is an ongoing challenge, especially as technology changes and adversaries adapt their tactics. The costs—e.g., legal, monetary, and reputational—of cyberattacks that hurt businesses are rising with little to no end in sight. The Chamber would like to see U.S. cybersecurity efforts reach the point in which stakeholders are stopping impending attacks or ending them extraordinarily quickly through the coordinated intelligence sharing and analysis, not just investigating them after the fact.

***

The Chamber welcomed the occasion to appear in April before the Cyber Forum. We would be pleased to join the body again to expand on the ideas in this letter and answer any questions.

The Chamber wants the interagency group to take away four overarching themes:

- The Chamber has been actively promoting the joint industry-NIST cybersecurity Framework since it was released in 2014. It is an excellent baseline for businesses' cybersecurity practices at home and internationally. The Chamber urges policymakers to help agencies streamline existing regulations with the Framework and maintain the Framework's dynamic, nonregulatory nature.

- The Chamber opposes creating new regulations, especially when government entities have not taken affected entities' perspectives into account. The FCC's proposed rulemaking on broadband privacy is a prime example. It retreats from the bottom-up, cooperative approach to cybersecurity policy. However, a course correction, leading to positive results, is still achievable. The Cyber Forum can influence this outcome.

- The Framework is part of a collection of important cybersecurity policy initiatives, including expanding voluntary threat data sharing and increasing adherence to international cyber norms and deterrence, which should advance together.

- Law enforcement entities, especially the FBI and the Secret Service, want to be an ally of industry, not an extension of regulatory agencies. U.S. and allied cybersecurity stakeholders need to build capacity to thwart attacks before they happen. Business spending on cybersecurity is increasing. Similar costs need to be imposed on bad actors.

If you have any questions or need more information, please do not hesitate to contact me (abeauchesne@uschamber.com; 202-463-3100) or my colleague Matthew J. Eggers (meggers@uschamber.com; 202-463-5619).

Sincerely,

Ann M. Beauchesne
Senior Vice President

Matthew J. Eggers
Executive Director, Cybersecurity Policy

Notes

[1] The three discussion topics are taken from the Cyber Forum's April 21, 2016, agenda.

[2] On February 9, 2016, the U.S. Chamber sent a letter to NIST, commenting on the Framework. Key points that the Chamber made in the letter include the following:

- The Chamber has been actively promoting the Framework.
- Chamber members are using the Framework and urging business partners to manage cybersecurity risks to their information networks and systems.
- The Chamber urges policymakers to help agencies and departments streamline existing regulations with the Framework and maintain the Framework's voluntary nature.
- Industry opposes creating new or quasi-cybersecurity regulations, particularly when government authorities have not taken affected entities' perspectives into account.

[3] See the Chamber-led March 11, 2016, group letter to the European Commission (EC). The EC requested stakeholders' views on cybersecurity public-private partnerships. The letter, signed by 19 industry associations, argues that embracing the Framework approach could advance the EU's goals for cybersecurity and a Digital Single Market.

[4] On June 14, 2016, the House Energy and Commerce Committee's Communications and Technology Subcommittee held a hearing titled *FCC Overreach: Examining the Proposed Privacy Rules*.

[5] See the Chamber Environment, Technology & Regulatory Affairs Department's May 26, 2016, letter to the FCC regarding the proposed broadband privacy rulemaking released on April 1, 2016.

[6] "Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks" (December 10, 2015). UC Davis *Business Law Journal*, 2016; Kelley School of Business Research Paper No. 16–2.

[7] The CSRIC IV report notes, "The sector's participation in CSRIC WG4 was seen as an opportunity to assume the leadership urged by FCC Chairman Tom Wheeler in a speech delivered to the American Enterprise Institute in June 2014" (pg. 4).

[8] Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute, Washington, D.C. (June 12, 2014). Also, the recent launch of a Commission proceeding to mandate that providers report on broadband network availability is another example of the FCC turning its back on the voluntary, public-private efforts and commitments undertaken in CSRIC IV and favoring regulation instead. See *Amendments to Part 4 of the*

Commission's Rules Concerning Disruption to Communications, Report and Order, *Further Notice of Proposed Rulemaking, and Order on Reconsideration*, PS Docket No. 15–80 (item released on May 26, 2016).

[9] Charter of the Cybersecurity Forum for Independent and Executive Branch Regulators (Cyber Forum charter), pg. 1.

[10] The 2015 cyber legislation was included in the Consolidated Appropriations Act, 2016 (P.L. 114-113).

[11] House Homeland Security Committee's Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee hearing, *Oversight of the Cybersecurity Act of 2015* (June 15, 2016).

[12] See the July 20, 2015, Chamber-led multiassociation letter to the U.S. Bureau of Industry and Security.

[13] "Wassenaar negotiators warming to industry's arguments," *Politico* Morning Cybersecurity (June 24, 2016).

[14] "Obama administration agrees to renegotiate cyber export controls," *Inside Cybersecurity* (February 29, 2016).

[15] "On cyber threats, who you gonna call?" *Washington Examiner* (May 9, 2016), pg. 7. Also, "FBI director pledges confidentiality as he urges reporting of data breaches," *Inside Cybersecurity* (April 26, 2016).

[16] "DOJ official: Hacked companies face unwarranted blame," *Inside Cybersecurity* (May 27, 2015).

[17] Cyber Forum charter, pg. 2.

[18] See *The United States Government Manual, 2015*.

[19] "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats," *Harvard National Security Journal*, Volume 7, Issue 2 (June 20, 2016). Listen to "The Lawfare Podcast: John Carlin Uses All the Tools" (July 2, 2016).

[20] According to the Chamber's June 8, 2016, policy statement on cybersecurity norms and deterrence, we generally agrees with the administration's 2015 policy regarding cyber deterrence. The administration prioritizes deterring cyberattacks that threaten the loss of life and critical infrastructure systems and services, which would likely be equated as acts of war under international law.

But the cyber deterrence report is incomplete. The Chamber believes that the administration's statement on deterrence, while taking many positive steps, does not adequately address the gap that exists between (1) major cyber incidents, which have not occurred yet, and (2) the more frequent, relatively minor attacks (e.g., pings) launched by unsophisticated actors that companies are capable of blunting mostly on their own and/or with the assistance of outside service providers.

Thus, in the *malicious middle* of the spectrum are costly attacks against businesses that are linked to criminal groups and foreign powers or their surrogates that will virtually never be deterred, much less punished. National governments are either too slow, underresourced, or not well organized in cyberspace to respond fast and effectively. Costs—true calculus-changing costs that would alter the behavior of would-be attackers—are rarely imposed on bad actors.