From: **Anne Hobson**
Date: Mon, Apr 10, 2017 at 9:23 AM
Subject: NIST Comments
To: cyberframework@nist.gov

To Whom It May Concern:

I have attached the R Street Institute's comments to NIST regarding the Cybersecurity Framework Version 1.1. Please confirm receipt of these comments.

Sincerely,
Anne Hobson

--
Anne Hobson
Tech Policy Fellow
R Street Institute

[Attachment Copied Below]

Before the
National Institute of Standards and Technology
Washington, D.C.

In the Matter of	)
	)
The Request for Comments	)
On the 2017 draft	)
Framework for Improving	)
Critical Infrastructure	)
Cybersecurity Version 1.1	)

COMMENTS OF THE R STREET INSTITUTE

April 10, 2017

Prepared by:
Anne Hobson
Technology Policy Fellow
R Street Institute
1050 17th St. NW #1150, Washington, D.C., 20036

Introduction

On behalf of the R Street Institute, we respectfully submit these comments to the National Institute of Standards and Technology on the Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 [hereinafter "the Framework"].[1] The R Street Institute is a free-market think tank with a pragmatic approach to public-policy challenges.

We thank NIST for the opportunity for further comment on the scope and efficacy of the most recent version of the Framework. We are encouraged to see an updated draft include supply-chain risk management and tools to measure cyber risk. The Framework serves as a common language for stakeholders with interest in cybersecurity—from insurers to manufacturers. Our comments focus on a selection of the questions posed by NIST, including topics not yet addressed (question 1); the labeling of the Framework itself (question 6); and areas that should be added to the NIST Roadmap for Improving Critical Infrastructure Cybersecurity [hereinafter "the Roadmap"] [2] (question 7).

---

[1] National Institute of Standards and Technology, "Cybersecurity Framework Draft Version 1.1," Cybersecurity Framework, Jan. 10, 2017. https://www.nist.gov/cyberframework/draft-version-11

[2] National Institute of Standards and Technology, "Cybersecurity Framework Workshop 2016," April 6 and 7, 2016. https://www.nist.gov/news-events/events/2016/04/cybersecurity-framework-workshop-2016

I. Additional Topics and Areas

In response to questions 1 and 7,[3] cyber insurance should be addressed in the final draft and would be a worthwhile addition to the Roadmap for future areas for improvement. Cyber-insurance coverage is an important aspect of the Framework's "recovery" function. Prompting users to consider cyber-insurance adoption as part of the enterprise risk management process could help raise the bar for device security, bolstering the global cybersecurity ecosystem.

In 2013, the White House published a list of proposed incentives to encourage adoption of the Framework. They highlighted cyber insurance as one incentive area, suggesting that NIST work closely with the insurance industry to ensure the Framework can complement underwriting practices to "foster a competitive cyber-insurance market."[4] This can have spillover benefits for cybersecurity, especially in industries with low adoption rates. Currently, less than 5 percent of the manufacturing sector has cyber-insurance coverage while the cyber-insurance takeup rate in the retail, health and financial services sectors is around 80 percent.[5] Nevertheless, manufacturing is among the top five industries targeted by cyberattacks in 2015, along with health care, financial services, government and transportation.[6]

NIST itself has recognized the role cyber insurance can play in helping businesses respond to and recover from a cyber incident.[7] In NIST Special Publication 800-184, insurers are one of the external parties emphasized to play a role in cybersecurity event recovery.[8] Cyber insurance was the subject of a panel at NIST's workshop in April 2016.[9] The workshop revealed that insurers are using the Framework to improve the underwriting process and the products and pricing they make available. Not only does cyber insurance help companies plan for risks, but insurers also are referencing the Framework to perform risk assessments that can help companies understand their vulnerabilities and communicate with clients about cyber preparedness. Because the Framework is comprehensive, it allows insurers to understand an organization's risk management "security culture."

---

[2] National Institute of Standards and Technology, "Cybersecurity Framework Workshop 2016," April 6 and 7, 2016. https://www.nist.gov/news-events/events/2016/04/cybersecurity-framework-workshop-2016

[3] Question 1: Are there any topics not addressed in the draft Framework Version 1.1 that could be … addressed in the final? Question 2: Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

[4] Michael Daniel, "Incentives to Support Adoption of the Cybersecurity Framework," White House Blog, Aug. 6, 2013. https://obamawhitehouse.archives.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework

[5] Council of Insurance Agents and Brokers, "Cyber-insurance Market Watch Survey," October 2016. https://www.ciab.com/uploadedFiles/Resources/Cyber_ Survey/102016CyberSurvey_Final.pdf

[6] IBM X-Force Research, "IBM 2016 Cyber Security Intelligence," 2016. https://www-03.ibm.com/security/data-breach/threat-intelligence-index.html

[7] National Institute of Standards and Technology, "Small Business Information Security: The Fundamentals," NISTIR 7621 Rev. 1, November 2016, 26-27. https://doi.org/10.6028/NIST.IR.7621r1

[8] Michael Bartock et al., "Guide for Cybersecurity Event Recovery," NIST SP 800-184, December 2016, 12. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

[9] National Institute of Standards and Technology, "Cybersecurity Framework Workshop 2016," April 7, 2017. https://www.nist.gov/news-events/events/2016/04/cybersecurity-framework-workshop-2016

In the case of a cyberattack, insurers also aid by investigating and reporting the incident. Cyber-insurance policies sometimes include coverage for breach-response costs; breach notification to consumers; credit monitoring; call centers; technical forensic investigations; public relations services; distributed denial of service mitigation services; regulatory fines; and legal defense and settlement costs.[10]

Including cyber insurance in the Framework will promote adoption, raise the quality of risk-based products and increase the availability and affordability of insurance products. Combating issues related to cybersecurity and privacy will require efforts from industry, policymakers, consumers and third parties. By including cyber insurance both in the Roadmap under "Areas for Development, Alignment and Collaboration" and in the Framework under the "Recover" function, NIST can play a role in supporting broader adoption of cyber-insurance coverage to mitigate risks associated with cyberattacks.

II. Reframing the Framework

Question 6 asks about the labeling of this version of the Framework.[11] While the version title "1.1" is salient, the longer title "Framework for Improving Critical Infrastructure Cybersecurity" is misleading. Functionally, the Framework is not limited to critical-infrastructure applications. In fact, it is useful for any organization seeking to manage its cyber risk, not just those in the federally designated critical-infrastructure sectors. Removing "critical infrastructure" from the title will signal that this is a generally applicable guidance document that offers resources to companies at every stage of cybersecurity policy development. Framing this document more broadly could lead to wider adoption among small businesses and organizations in the United States and abroad.

The Framework was developed in response to Executive Order 13636 "Improving Critical Infrastructure Cybersecurity," which envisioned two goals–to secure the nation's critical infrastructure and to maintain a healthy cyber environment.[12] Since 2013, the Framework has evolved into a versatile and helpful tool for cyber-risk management. Users of the Framework include insurance companies, nonprofit organizations, universities, and small and large private companies in the United States and abroad. Packaging the framework as a cybersecurity resource for critical infrastructure limits its use.

In Version 1.1, NIST reiterates that use of the Framework is voluntary and encourages users to "customize the Framework to maximize organizational value."[13] It is important that the Framework remain voluntary for private transactions, precisely so organizations have the flexibility to customize it to their specific cybersecurity needs, priorities, resources and capabilities.

---

[10] Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World," R Street Institute Policy Study No. 86, February 2017. http://www.rstreet.org/policy-study/aligning-cybersecurity-incentives-in-an-interconnected-world/

[11] Question 6: Is there a better label than "version 1.1" for this update?

[12] White House "Improving Critical Infrastructure Cybersecurity," Exec. Order No. 13636, 78 Fed. Reg. 11737, Feb. 12, 2013. https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

[13] National Institute of Standards and Technology, "Cybersecurity Framework Draft Version 1.1," Cybersecurity Framework, January 10, 2017. https://www.nist.gov/cyberframework/draft-version-11

Internet-enabled devices are diverse in function and nature. When design standards become requirements, they risk becoming overly complex or inadequate. NIST recognizes this in the Framework: "Diverse or specialized requirements can impede interoperability, result in duplication, harm cybersecurity and hinder innovation."[14] In the volatile cybersecurity battlefield, standards also can easily become outdated. If codified in a formal industrywide regulation, standards may be difficult to change over time. Such requirements would crowd out private efforts to improve cybersecurity at the industry and firm level. Finally, the costs to comply with such requirements could deter innovation in the internet of things[15]—an emerging sector that could generate between $3.9 and $11.1 trillion per year by 2025, equivalent to up to 11 percent of the global economy.[16] Internet-of-things technologies are transforming infrastructure, agriculture, energy, transportation, manufacturing, health and communications, among other sectors,[17] as connected devices make us more productive and prosperous.

Promoting an open global environment to develop internet-enabled technology is paramount for continued U.S. leadership in the global economy. While the Framework references globally recognized standards and can be applied in organizations abroad, it ultimately is an American effort led by the U.S. Commerce Department. This is both a challenge and a strength, as some countries are hesitant to accept U.S. guidance. The Framework could serve as the basis for a global conversation about an open-source set of standards as a resource for organizations worldwide. The Commerce Department and NIST should take the lead in working with governments abroad to establish standards and norms in cybersecurity and a truly global voluntary framework. By reworking the title to address cybersecurity in organizations beyond critical infrastructure, by maintaining its voluntary nature and by emphasizing the Framework as a product of cooperation between stakeholders, the Commerce Department can best influence global practices.

Conclusion

We are encouraged by NIST's efforts so far to create a common language around cybersecurity practices for stakeholders. NIST should continue to seek out ways to convene stakeholders and encourage organizations to develop and adopt cybersecurity best practices voluntarily. As more devices and emerging technologies rely on internet connectivity, the Framework will serve as an important tool to empower organizations worldwide. We look forward to continuing to engage with NIST on this topic.

Respectfully submitted,
Anne Hobson
Technology Policy Fellow
R Street Institute

---

[14] National Institute of Standards and Technology, "NIST Roadmap for Improving Critical Infrastructure Cybersecurity," February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

[15] The internet of things is defined as an array of connected objects with unique identifiers that have the ability to transfer data over a network.

[16] James Manyika, et al., "Unlocking the Potential of the Internet of Things," McKinsey Global Institute, June 2015. http://www.mckinsey.com/business-functions/digitalmckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physicalworld

[17] Defined as an array of connected objects with unique identifiers that have the ability to transfer data over a network.