Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket Number: [140721609-4609-01**]**

Experience with the Framework for Improving Critical Infrastructure Cybersecurity

AGENCY: National Institute of Standards and Technology, U.S. Department of Commerce.

ACTION: Notice; Request for Information (RFI).

SUMMARY: The National Institute of Standards and Technology (NIST) requests information about the level of awareness throughout critical infrastructure organizations, and initial experiences with the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"). As directed by Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (the "Executive Order"), the Framework consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Framework was released on

February 12, 2014, after a year-long, open process involving private and public sector organizations, including extensive input and public comments.

Responses to this RFI – which will be posted at http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm – will inform NIST's planning and decision-making about possible tools and resources to help organizations to use the Framework more effectively and efficiently. They will also help inform future versions of the Framework. The responses will also inform the Department of Homeland Security's Critical Infrastructure Cyber Community C^3 Voluntary Program. In addition, NIST is interested in receiving comments related to the Roadmap that accompanied publication of the Framework. All information provided will also assist in developing the agenda for a workshop on the Framework being planned for October 2014.

DATES: Comments must be received by 5:00 PM Eastern time on [INSERT DATE 45 DAYS AFTER FEDERAL REGISTER PUBLICATION].

ADDRESSES: Written comments may be submitted by mail to Diane Honeycutt, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899. Online submissions in electronic form may be sent to cyberframework@nist.gov in any of the following formats: HTML; ASCII; Word; RTF; or PDF. Please submit comments only and include your name, organization's name (if any), and cite "Experience with the Framework for Improving Critical Infrastructure Cybersecurity" in all correspondence. Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials.

All comments received in response to this RFI will be posted at http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information).

FOR FURTHER INFORMATION CONTACT: For questions about this RFI contact: Adam Sedgewick, U.S. Department of Commerce, 1401 Constitution Avenue, NW, Washington, DC 20230, telephone (202) 482–0788, e-mail Adam.Sedgewick@nist.gov. Please direct media inquiries to NIST's Office of Public Affairs at (301) 975-2762.

SUPPLEMENTARY INFORMATION:

The national and economic security of the United States depends on the reliable functioning of critical infrastructure,[1] which has become increasingly dependent on information technology. Recent cyber attacks and publicized weaknesses reinforce the need for improved capabilities for defending against malicious cyber activity. This will be a long-term challenge. Additional steps must be taken to enhance existing efforts to increase the protection and resilience of critical infrastructure, while maintaining a cyber

[1] For the purposes of this RFI the term "critical infrastructure" has the meaning given the term in 42 U.S.C. 5195c(e): "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

environment that encourages efficiency, innovation, and economic prosperity while also protecting privacy and civil liberties.

By Executive Order,[2] the Secretary of Commerce was tasked to direct the Director of the National Institute of Standards and Technology (NIST) to lead the development of a voluntary framework to reduce cyber risks to critical infrastructure (the "Framework").[3] The Framework consists of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks. The Framework was developed by NIST using information collected through the RFI that was published in the Federal Register on February 25, 2013, a series of open public workshops, and a 45-day public comment period announced in the Federal Register on October 29, 2013. It was published on February 12, 2014, after a year-long, open process involving private and public sector organizations, including extensive input and public comments, and announced in the Federal Register (79 FR 9167) on February 18, 2014.

Given the diversity of sectors in the Nation's critical infrastructure, the Framework development process was designed to build on cross-sector security standards and guidelines that are immediately applicable or likely to be applicable to critical infrastructure, to increase visibility and adoption of those standards and guidelines, and to find potential areas for improvement (i.e., where standards/guidelines are nonexistent or

[2] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 FR 11739 (February 19, 2013).

[3] https://www.federalregister.gov/articles/2014/02/18/2014-03495/ cybersecurity-framework

where existing standards/guidelines are inadequate) that need to be addressed through future collaboration with industry and industry-led standards bodies. The Cybersecurity Framework incorporates voluntary consensus standards and industry best practices to the fullest extent possible and is consistent with voluntary international consensus-based standards when such international standards advance the objectives of the Executive Order. The Framework is designed for compatibility with existing regulatory authorities and regulations, although it is intended for voluntary adoption.

While the focus of the Framework is on the Nation's critical infrastructure, it was developed in a manner to promote wide adoption of practices to increase risk management-based cybersecurity across all industry sectors and by all types of organizations.

NIST remains committed to helping organizations understand and use the Framework. In the five-plus months since the document was published, NIST has reached out and responded to a large number of organizations to raise awareness, answer questions, and learn about their experiences with the Framework.

NIST has worked closely with industry groups, associations, non-profits, government agencies, and international standards bodies to increase awareness of the Framework. NIST has promoted the use of the Framework as a basic, flexible, and adaptable tool for managing and reducing cybersecurity risks, most frequently working in partnership with leaders at all levels of stakeholder organizations.

While the initial focus was on cross-sector needs, Section 8(b) of the Executive Order called on "Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments." NIST has participated in these and similar industry-government collaborative activities, in some cases serving in an advisory capacity.

In the time since the Framework's publication, NIST's primary goal has been to raise awareness of the Framework and how it can be used to manage cyber risks, in order to assist industry sectors and organizations to gain experience with it. While NIST appreciates that widespread implementation of the Framework can only occur over time, NIST views extensive voluntary use as critical to achieving the goals of the Executive Order. For these reasons, NIST is interested in learning about individual companies' and other organizations' knowledge of and experiences with the Framework. NIST wants to better understand how companies and organizations in all critical infrastructure sectors are approaching and making specific use of the Framework, in accordance with Section 7(f) of the Executive Order. This includes learning about which aspects of the Framework have been helpful or challenging, and about whether and how the Framework has been used to modify and strengthen management of cyber risks. The RFI responses will also inform the Department of Homeland Security's Critical Infrastructure Cyber Community C³ Voluntary Program.[4]

[4] http://www.us-cert.gov/ccubedvp

NIST understands that at this early stage the Framework may be used in a variety of ways, including: participation in a sector group that is reviewing how the Framework can best be implemented and coordinated with ongoing or planned initiatives; initial high-level review of an organization's current management of cyber risk; and more intensive deployment as an organization's guiding approach to managing its cyber risk.

In addition to seeking comments from individual critical infrastructure owners and operators of all sizes and their representatives from sector and professional associations, NIST invites submissions from Federal agencies, state, local, territorial and tribal governments, standard-setting organizations,[5] other members of industry, consumers, solution providers, and other stakeholders.

REQUEST FOR INFORMATION

The following questions cover the major areas about which NIST seeks comment. They are not intended to limit the topics that may be addressed. Responses may include any topic believed to have implications for the degree of awareness and voluntary use and subsequent improvement of the Framework, regardless of whether the topic is included in this document.

[5] As used herein, "standard-setting organizations" refers to the wide cross section of organizations that are involved in the development of standards and specifications, both domestically and abroad.

While the Framework and associated outreach activities by NIST have focused on critical infrastructure, given the broad diversity of sectors that may include parts of critical infrastructure and the intention to continue to involve a broad set of stakeholders in use and evolution of the Framework, the RFI generally uses the broader term "organizations" in seeking information. NIST is especially interested in comments that will help to determine the Framework's usefulness and potential applicability across all critical infrastructure sectors. In addition, considering the interwoven nature of our Internet-based economy and society, information from and about organizations not included in critical infrastructure sectors also will be valuable.

Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Do not include in comments or otherwise submit proprietary or confidential information, as all comments received in response to this RFI will be made available publically at http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm.

Current Awareness of the Cybersecurity Framework

Recognizing the critical importance of widespread voluntary usage of the Framework in order to achieve the goals of the Executive Order, and that usage initially depends upon awareness, NIST solicits information about awareness of the Framework and its intended uses among organizations.

1. What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it

gained the traction needed to be a factor in how organizations manage cyber risks in the Nation’s critical infrastructure?

2. How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?
3. Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?
4. Is there general awareness that the Framework:
   a. Is intended for voluntary use?
   b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?
   c. Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?
5. What are the greatest challenges and opportunities – for NIST, the Federal government more broadly, and the private sector – to improve awareness of the Framework?
6. Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?
7. If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?

8. Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?
9. What more can and should be done to raise awareness?

Experiences with the Cybersecurity Framework

NIST is seeking information on the experiences with, including but not limited to early implementation and usage of, the Framework throughout the Nation's critical infrastructure. NIST seeks information from and about organizations that have had direct experience with the Framework. Please provide information related to the following:

1. Has the Framework helped organizations understand the importance of managing cyber risk?
2. Which sectors and organizations are actively planning to, or already are, using the Framework, and how?
3. What benefits have been realized by early experiences with the Framework?
4. What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?
5. Do organizations in some sectors require some type of sector specific guidance prior to use?

6. Have organizations that are using the Framework integrated it with their broader enterprise risk management program?
7. Is the Framework's approach of major components – Core, Profile, and Implementation Tiers – reasonable and helpful?
8. Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.
    a. Of these recommended practices, how are organizations initially using the Framework?
    b. Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?
    c. Are organizations leveraging Section 3.5 of the Framework ("Methodology to Protect Privacy and Civil Liberties") and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?
    d. Are organizations changing their cybersecurity governance as a result of the Framework?
    e. Are organizations using the Framework to communicate information about their cybersecurity risk management programs – including the effectiveness of those programs – to stakeholders, including boards, investors, auditors, and insurers?
    f. Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?

9. Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?
10. Have organizations developed practices to assist in use of the Framework?

Roadmap for the Future of the Cybersecurity Framework

NIST published a Roadmap[6] in February 2014 detailing some issues and challenges that should be addressed in order to improve future versions of the Framework. Information is sought to answer the following questions:

1. Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?
2. Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?
3. Have there been significant developments – in the United States or elsewhere – in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?

Dated: August 21, 2014.

Willie E. May
Associate Director for Laboratory Programs

[FR Doc. 2014-20315 Filed 08/25/2014 at 8:45 am; Publication Date: 08/26/2014]

[6] http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf