Billing Code 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice, request for comments.

SUMMARY:The National Institute of Standards and Technology (NIST) requests comments on a proposed update to the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"). The voluntary Framework consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Framework was published on February 12, 2014, after a year-long, open process involving private and public sector organizations, including extensive input and public comments. It has been used with increasing frequency and in a variety of ways by organizations of all sizes, areas of interest, and based inside and outside the United States. This Request for Comments (RFC) is meant to facilitate coordination with, "private sector personnel and entities, critical infrastructure owners and operators, and other relevant

industry organizations" as directed by the Cybersecurity Enhancement Act of 2014.[1] The proposed update to the Framework is available for review at http://www.nist.gov/cyberframework. Responses to this RFC will be posted at http://www.nist.gov/cyberframework and will inform NIST's planned update to the Framework.

DATES: Comments must be received by 5:00 p.m. Eastern time on April 10, 2017.

ADDRESSES: Written comments may be submitted by mail to Edwin Games, 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 "Comments on Draft Update of 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. The proposed update to the Framework is available for review at http://www.nist.gov/cyberframework.

[1] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

All comments received in response to this RFC will be posted at http://www.nist.gov/cyberframework without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information). Comments that contain profanity, vulgarity, threats, or other inappropriate language will not be posted or considered.

FOR FURTHER INFORMATION CONTACT: For questions about this RFC contact: Adam Sedgewick, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230, telephone (202) 482-0788, email 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,[2] which has become increasingly dependent on information technology. Cyber attacks and publicized weaknesses reinforce the need for improved capabilities for defending against malicious cyber activity. This is a long-term challenge. The Secretary of Commerce was tasked to direct the Director of NIST to lead the development of a voluntary framework to reduce cyber risks to critical infrastructure (the

[2] For the purposes of this RFC 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."

"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 Request for Information (RFI) that was published in the Federal Register on February 25, 2013 (78 FR 13024), a series of open public workshops, and a 45-day public comment period announced in the Federal Register on October 29, 2013 (78 FR 64478). 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 on February 18, 2014 (79 FR 9167). Responses to subsequent RFIs, as announced through the Federal Register (79 FR 50891 and 80 FR 76934), and workshops encouraged NIST to update the Framework.

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 Cybersecurity Enhancement Act of 2014. The Framework is designed for compatibility with existing regulatory authorities and regulations, although it is intended for voluntary adoption. 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

[3] *See* Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. The Cybersecurity Framework may be found at: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

that are immediately applicable or likely to be applicable to critical infrastructure. The process also was intended to increase visibility and use of those standards and guidelines, and to find potential areas for improvement (e.g., where standards/guidelines are nonexistent) that need to be addressed through future collaboration with industry and industry-led standards bodies.

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 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. The Framework was designed as a communication tool. It is applicable for leaders at all levels of an organization. For these reasons, NIST has engaged a wide diversity of stakeholders in Framework education. NIST has also issued several RFIs, held workshops, and encouraged direct communication with potential and current users of the Framework.

Based on the information received from the public via these channels and the work that it has carried out on cybersecurity – including its collaborative efforts with the private sector – NIST has developed a draft update of the Framework (termed "Version 1.1" or "V1.1"), available at http://www.nist.gov/cyberframework. This draft update seeks to clarify, refine,

and enhance the Framework, and make it easier to use, while retaining its flexible, voluntary, and cost-effective nature. The update also will be fully compatible with the February 2014 version of the Framework in that either version may be used by organizations without degrading communication or functionality.

Request for Comments

NIST is soliciting public comments on this proposed update. Specifically, NIST is interested in comments that address updated features of the Framework. These features seek to:

- Clarify Implementation Tier use and relationship to Profiles,
- Enhance guidance for applying the Framework for supply chain risk management,
- Provide guidance on metrics and measurements using the Framework,
- Update the FAQs to support understanding and use of Framework, and
- Update the Informative References.

NIST also will consider comments on other aspects of the Framework update.

All comments will be made available to the public. These comments will be analyzed and will be one focus of a public workshop to be held in May 2017. Details about that workshop, which also will feature user experiences with the Framework, will be announced on the NIST Cybersecurity Framework website at: https://www.nist.gov/cyberframework. To receive notice about the workshop, please contact: cyberframework@nist.gov.

After the May 2017 workshop and considering the comments received on this draft update, NIST intends to issue a final version of Framework V1.1 along with an updated Roadmap[4] document that describes recommended activities in work areas that are related and complimentary to the Framework.

Kevin Kimball
NIST Chief of Staff

[4] The Cybersecurity Framework Roadmap may be found at: https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf.

[FR Doc. 2017-01599 Filed: 1/24/2017 8:45 am; Publication Date: 1/25/2017]