Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number 151103999-6076-02]

Views On The Framework For Improving Critical Infrastructure Cybersecurity

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice; Extension of Comment Period

SUMMARY:

The National Institute of Standards and Technology (NIST) is extending the period for submitting comments relating to the "Framework for Improving Critical Infrastructure Cybersecurity" (the "Framework") through February 23, 2016. In a Request for Information (RFI) that published in the Federal Register on December 11, 2015 (80 FR 76934), NIST requested information about the variety of ways in which the Framework is being used to improve cybersecurity risk management, how best practices for using the Framework are being shared, the relative value of different parts of the Framework, the possible need for an update of the Framework, and options for the long-term governance

of the Framework. NIST is extending the comment period announced in the December 11, 2015 RFI from February 9, 2016 to February 23, 2016.

DATES:

Comments must be received by 5:00 p.m. Eastern time on February 23, 2016. Comments received after February 9, 2016 and before publication of this notice are deemed to be timely.

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 include your name and your organization's name (if any), and cite "Views on 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. Please do not submit additional 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: Diane Honeycutt, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899 or *cyberframework@nist.gov*. Please direct media inquiries to NIST's Office of Public Affairs at (301) 975-2762.

SUPPLEMENTARY INFORMATION:

NIST is extending the comment period announced in the December 11, 2015 Request for Information (RFI) (80 FR 76934) through February 23, 2016. NIST is authorized by the Cybersecurity Enhancement Act of 2014[1] to "facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure."[2] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" [3] tasked the Secretary of Commerce to direct the Director of NIST to lead the development of a framework to reduce cyber risks to critical infrastructure. A final version of Framework 1.0 was published on February 12, 2014, after a year-long, open process involving private and public sector organizations, including extensive industry input and public comments, and announced in the Federal Register (79 FR 9167) on

[1] Pub. L. No. 113-274 (2014): http://www.gpo.gov/fdsys/pkg/PLAW-113publ274/pdf/PLAW-113publ274.pdf

[2] *Id.*, codified in relevant part at 15 U.S.C. 272(c)(15). Congress's intent was to codify NIST's role in Executive Order No. 13636: "Title I would codify certain elements of Executive Order 13636 by directing the National Institute of Standards and Technology (NIST) to develop a framework of voluntary standards designed to reduce risks arising from cyberattacks on critical infrastructure that is privately owned and operated." S. Rep. No. 113-270, at 9 (2014).

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

February 18, 2014. On December 11, 2015 NIST published a RFI in the Federal Register (80 FR 76934) seeking information about the variety of ways in which the Framework is being used to improve cybersecurity risk management, how best practices for using the Framework are being shared, the relative value of different parts of the Framework, the possible need for an update of the Framework, and options for the long-term governance of the Framework. NIST is extending the comment period announced in the December 11, 2015 RFI from February 9, 2016 to February 23, 2016 to allow comments to be submitted during a timeframe in which a variety of cybersecurity events are scheduled to occur.

Kevin Kimball,
Chief of Staff.
[FR Doc. 2016-02860 Filed: 2/11/2016 8:45 am; Publication Date: 2/12/2016]