

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 130909789-4078-02]

Cybersecurity Framework

AGENCY: National Institute of Standards and Technology (NIST), Department of Commerce.

ACTION: Notice.

SUMMARY: This notice announces the issuance of the Cybersecurity Framework (the “Cybersecurity Framework” or “Framework”). The Framework was developed by NIST using information collected through the Request for Information (RFI) that was published in the Federal Register on February 26, 2013, a series of open public workshops, and a 45-day public comment period announced in the Federal Register on October 29, 2013.

The Framework was developed in response to NIST responsibilities directed in Executive Order 13636, “Improving Critical Infrastructure Cybersecurity” (“Executive Order”). Under the Executive Order, the Secretary of Commerce is tasked to direct the Director of NIST to lead the development of a framework to reduce cyber risks to critical infrastructure. The Framework consists of standards, methodologies, procedures and processes that align policy, business, and

technological approaches to address cyber risks. The Framework is available electronically from the NIST Web site at: <http://www.nist.gov/cyberframework>.

DATES: The Cybersecurity Framework was published on February 12, 2014.

ADDRESSES: The Cybersecurity Framework is available electronically from the NIST Web site at: <http://www.nist.gov/cyberframework>.

FOR FURTHER INFORMATION CONTACT: Diane Honeycutt, telephone: 301-975-8443, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930 or via email: diane.honeycutt@nist.gov. Please direct media inquiries to NIST's Public Affairs Office at (301) 975-NIST.

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 trends demonstrate the need for improved capabilities for defending against malicious cyber activity. Such activity is increasing, and its consequences can range from theft through disruption to destruction. Steps must be taken to enhance existing efforts to increase the protection and resilience of this infrastructure, while maintaining a cyber environment that encourages efficiency, innovation, and economic prosperity, while protecting privacy and civil liberties.

¹ For the purposes of this notice 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.”

Under the Executive Order,² the Secretary of Commerce is tasked to direct the Director of NIST to lead the development of a framework to reduce cyber risks to critical infrastructure (the “Cybersecurity Framework” or “Framework”). The Cybersecurity Framework consists of standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks. Given the diversity of sectors in critical infrastructure, the Framework development process was designed to initially identify 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 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 Cybersecurity Framework is designed for compatibility with existing regulatory authorities and regulations.

The Cybersecurity Framework provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls to help owners and operators of critical infrastructure and other interested entities to identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties. To enable technical innovation and account for organizational differences, the Cybersecurity Framework does not prescribe particular technological solutions or specifications. It includes guidance for measuring the performance of an entity in implementing the Cybersecurity Framework and includes methodologies to identify and mitigate impacts of the

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

Framework and associated information security measures and controls on business confidentiality and to protect individual privacy and civil liberties.

As a non-regulatory Federal agency, NIST developed the Framework in a manner that is consistent with its mission to promote U.S. innovation and industrial competitiveness through the development of standards and guidelines in consultation with stakeholders in both government and industry. The Framework provides owners and operators of critical infrastructure the ability to implement security practices in the most effective manner while allowing organizations to express requirements to multiple authorities and regulators. Issues relating to harmonization of existing relevant standards and integration with existing frameworks were also considered. While the focus is on the Nation's critical infrastructure, the Framework was developed in a manner to promote wide adoption of practices to increase cybersecurity across all sectors and industry types.

The Framework was developed through an open public review and comment process that included information collected through a Request for Information (RFI), a series of public workshops, and a 45-day public comment period on the preliminary version of the Cybersecurity Framework (“preliminary Framework”).

NIST published the RFI in the Federal Register (78 FR 13024) on February 26, 2013.³ Comments received in response to the RFI are available at

http://csrc.nist.gov/cyberframework/rfi_comments.html.

NIST held five open public workshops to provide the public with additional opportunities to

³ <https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity>

provide input. The first workshop was conducted on April 3, 2013, at the Department of Commerce in Washington, D.C. The second workshop was conducted on May 29-31, 2013, at Carnegie Mellon University in Pittsburgh, Pennsylvania. The third workshop was conducted on July 10-12, 2013, at the University of California, San Diego. The fourth workshop was conducted on September 11-13, 2013, at the University of Texas at Dallas. The fifth workshop was conducted on November 14-15, 2013, at the North Carolina State University in Raleigh, North Carolina. Agenda, discussion materials, and presentation slides for each of these workshops are available at <http://www.nist.gov/cyberframework/cybersecurity-framework-events.cfm>.

NIST issued the preliminary Framework and announced a 45-day public comment period in the Federal Register (78 FR 64478) on October 29, 2013.⁴ Comments received in response to the public comment period on the preliminary Framework are available at http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html.

Throughout the process, NIST issued public updates on the development of the Cybersecurity Framework. NIST issued the first update on June 18, 2013, and it is available at http://www.nist.gov/itl/upload/nist_cybersecurity_framework_update_061813.pdf.

NIST issued the second update on July 24, 2013, and it is available at <http://www.nist.gov/itl/upload/NIST-Cybersecurity-Framework-Update-072413.pdf>.

NIST issued the third update on December 4, 2013, and it is available at http://www.nist.gov/itl/upload/nist_cybersecurity_framework_update_120413.pdf.

NIST issued the fourth update on January 15, 2014, and it is available at <http://www.nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-Update-011514->

⁴ <https://www.federalregister.gov/articles/2013/10/29/2013-25566/request-for-comments-on-the-preliminary-cybersecurity-framework>

[2.pdf](#). The fourth update was issued after the conclusion of the public comment period for the preliminary Framework and highlights major themes reflected in the submissions, along with NIST's responses to these comments.

The Framework incorporates existing consensus-based standards to the fullest extent possible, consistent with requirements of the National Technology Transfer and Advancement Act of 1995,⁵ and guidance provided by Office of Management and Budget Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities."⁶ Principles articulated in the Executive Office of the President memorandum M-12-08 "Principles for Federal Engagement in Standards Activities to Address National Priorities"⁷ are followed. The Framework is also consistent with, and supported by the broad policy goals of, the Administration's 2010 "National Security Strategy,"⁸ 2011 "Cyberspace Policy Review,"⁹ "International Strategy for Cyberspace"¹⁰ of May 2011 and HSPD-7 "Critical Infrastructure Identification, Prioritization, and Protection."¹¹

Dated: February 11, 2014.

Patrick Gallagher,
Under Secretary of Commerce for Standards and Technology.

[FR Doc. 2014-03495 Filed 02/14/2014 at 8:45 am; Publication Date: 02/18/2014]

⁵ Public Law 104-113 (1996), codified in relevant part at 15 U.S.C 272(b).

⁶ http://www.whitehouse.gov/omb/circulars_a119

⁷ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf>

⁸ http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

⁹ http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

¹⁰ http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

¹¹ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m-04-15.pdf>