Billing Code: 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Multistakeholder Process on Internet of Things Security Upgradability and Patching

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice of Open Meeting.

SUMMARY: The National Telecommunications and Information Administration (NTIA) will convene a virtual meeting of a multistakeholder process concerning Internet of Things Security Upgradability and Patching on January 31, 2017.

DATES: The meeting will be held on January 31, 2017, from 2:00 p.m. to 4:30 p.m., Eastern Time.

ADDRESSES: This is a virtual meeting. NTIA will post links to online content and dial-in information on the multistakeholder process website at https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

FOR FURTHER INFORMATION CONTACT: Allan Friedman, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW, Room 4725, Washington, DC 20230; telephone: (202) 482-4281; email: afriedman@ntia.doc.gov. Please direct media inquiries to NTIA's Office of Public Affairs: (202) 482-7002; email: press@ntia.doc.gov.

SUPPLEMENTARY INFORMATION:

Background: In March of 2015 the National Telecommunications and Information Administration issued a Request for Comment to "identify substantive cybersecurity issues that

affect the digital ecosystem and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers."[1] We received comments from a range of stakeholders, including trade associations, large companies, cybersecurity startups, civil society organizations and independent computer security experts.[2] The comments recommended a diverse set of issues that might be addressed through the multistakeholder process, including cybersecurity policy and practice in the emerging area of Internet of Things (IoT). On August 2, 2016, NTIA announced that it would convene a new multistakeholder process on security upgradability and patching for consumer IoT.[3] NTIA subsequently announced that the first meeting of this process would be held on October 19, 2016.[4]

The matter of patching vulnerable systems is now an accepted part of cybersecurity.[5] Unaddressed technical flaws in systems leave the users of software and systems at risk. The nature of these risks varies, and mitigating these risks requires various efforts from the

[1] U.S. Department of Commerce, Internet Policy Task Force, Request for Public Comment, Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 Fed. Reg. 14360, Docket No. 150312253-5253-01 (Mar. 19, 2015), *available at*: https://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf.

[2] NTIA has posted the public comments received at https://www.ntia.doc.gov/federal-register-notice/2015/comments-stakeholder-engagement-cybersecurity-digital-ecosystem.

[3] NTIA, Increasing the Potential of IoT through Security and Transparency (Aug. 2, 2016), *available at:* https://www.ntia.doc.gov/blog/2016/increasing-potential-iot-through-security-and-transparency.

[4] NTIA, Notice of Multistakeholder Process on Internet of Things Security Upgradability and Patching Open Meeting (Sept. 15, 2016), *available at:* https://www.ntia.doc.gov/federal-register-notice/2016/10192016-meeting-notice-msp-iot-security-upgradability-patching.

[5] *See, e.g.*, Murugiah Souppaya and Karen Scarfone, *Guide to Enterprise Patch Management Technologies, Special Publication 800-40 Revision 3*, National Institute of Standards and Technology, NIST SP 800-40 (2013) *available at*: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf.

developers and owners of these systems. One of the more common means of mitigation is for the developer or other maintaining party to issue a security patch to address the vulnerability. Patching has become more commonly accepted, even for consumers, as more operating systems and applications shift to visible reminders and automated updates. Yet as one security expert notes, this evolution of the software industry has yet to become the dominant model in IoT.[6]

To help realize the full innovative potential of IoT, users need reasonable assurance that connected devices, embedded systems, and their applications will be secure. A key part of that security is the mitigation of potential security vulnerabilities in IoT devices or applications through patching and security upgrades.

The ultimate objective of the multistakeholder process is to foster a market offering more devices and systems that support security upgrades through increased consumer awareness and understanding. Enabling a thriving market for patchable IoT requires common definitions so that manufacturers and solution providers have shared visions for security, and consumers know what they are purchasing. Currently, no such common, widely accepted definitions exist, so many manufacturers struggle to effectively communicate to consumers the security features of their devices. This is detrimental to the digital ecosystem as a whole, as it does not reward companies that invest in patching, and it prevents consumers from making informed purchasing choices.

At the October 19, 2016, meeting, stakeholders discussed the challenge of patching, and how to scope the discussion. Participants identified five distinct work streams that could help foster better security across the ecosystem, and established working groups to more fully

[6] Bruce Schneier, *The Internet of Things Is Wildly Insecure — And Often Unpatchable*, Wired (Jan. 6, 2014) *available at:* https://www.schneier.com/blog/archives/2014/01/security_risks_9.html.

evaluate options in each of these areas.[7] The main objective of the January 31, 2016, meeting is to share progress from the working groups examining the five work streams, and hear feedback from the broader stakeholder community. Stakeholders will also discuss overall progress on the initiative, and identify any additional work that may be needed.

More information about stakeholders' work will be available at: https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

Time and Date: NTIA will convene a virtual meeting of the multistakeholder process on IoT Security Upgradability and Patching on January 31, 2017, from 2:00 p.m. to 4:30 p.m., Eastern Time. Please refer to NTIA's website, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security, for the most current information.

Place: This is a virtual meeting. NTIA will post links to online content and dial-in information on the multistakeholder process website at https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

Other Information: The meeting is open to the public and the press. There will be an opportunity for stakeholders viewing the webcast to participate remotely in the meetings through a moderated conference bridge, including polling functionality. Access details for the meetings are subject to change. Requests for a transcript of the meeting or other auxiliary aids should be directed to Allan Friedman at (202) 482-4281 or afriedman@ntia.doc.gov at least seven (7) business days prior to each meeting. Please refer to NTIA's website, http://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security, for the most current information.

[7] *See* NTIA, Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching, at: https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

Dated: January 11, 2017.

Kathy D. Smith,

Chief, National Telecommunications and Information Administration.
[FR Doc. 2017-00817 Filed: 1/13/2017 8:45 am; Publication Date: 1/17/2017]