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 meeting of a multistakeholder process on Internet of Things Security Upgradability and Patching on April 26, 2016.

DATES: The meeting will be held on April 26, 2017, from 10:00 a.m. to 4:00 p.m., Eastern Time. See Supplementary Information for details.

ADDRESSES: The meeting will be held at the American Institute of Architects, 1735 New York Ave., NW, Washington, DC 20006.

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).

In a separate but related matter in April 2016, NTIA, the Department's Internet Policy Task Force, and its Digital Economy Leadership Team sought comments on the benefits, challenges, and potential roles for the government in fostering the advancement of the IoT.[3] Over 130 stakeholders responded with comments addressing many substantive issues and opportunities related to IoT.[4] Security was one of the most common topics raised. Many commenters emphasized the need for a secure lifecycle approach to IoT devices that considers the development, maintenance, and end-of-life phases and decisions for a device.

[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] U.S. Department of Commerce, Internet Policy Task Force, Request for Public Comment, Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 Fed. Reg. 19956, Docket No 160331306-6306-01 (Apr. 5, 2016), *available at*: https://www.ntia.doc.gov/federal-register-notice/2016/rfc-potential-roles-government-fostering-advancement-internet-of-things.

[4] NTIA has posted the public comments received at https://www.ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things.

On August 2, 2016, after reviewing these comments, NTIA announced that the next multistakeholder process on cybersecurity would be on IoT security upgradability and patching.[5] NTIA subsequently announced that the first meeting of a multistakeholder process on this topic would be held on October 19, 2016.[6] A second, virtual meeting of this process was held on January 31, 2017.[7]

The matter of patching vulnerable systems is now an accepted part of cybersecurity.[8] 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 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.[9]

---

[5] 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.

[6] 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.

[7] NTIA, Notice of 01/31/2017 Meeting of the Multistakeholder Process on Internet of Things Security Upgradability and Patching (Jan. 11, 2017), *available at:* https://www.ntia.doc.gov/federal-register-notice/2017/notice-01312017-meeting-multistakeholder-process-internet-things.

[8] *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.

[9] 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.

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.

Stakeholders have identified four distinct work streams that could help foster better security across the ecosystem.[10] The main objectives of the April 26, 2017 meeting are to share progress from the working groups and hear feedback from the broader stakeholder community. Stakeholders will also discuss their vision of the timing and outputs of this initiative, and how the different work streams can complement each other.

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

Time and Date: NTIA will convene a meeting of the multistakeholder process on Internet of Things Security Upgradability and Patching on April 26, 2017, from 10:00 a.m. to 4:00 p.m., Eastern Time. The meeting date and time are subject to change. Please refer to NTIA's website,

[10] Documents shared by working group stakeholders are *available at*: https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security, for the most current information.

Place: The meeting will be held at the American Institute of Architects, 1735 New York Ave., NW, Washington, DC 20006. The location of the meeting is subject to change. Please refer to NTIA's website, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security, for the most current information.

Other Information: The meeting is open to the public and the press. The meeting is physically accessible to people with disabilities. Requests for sign language interpretation 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 the meeting. The meeting will also be webcast. Requests for real-time captioning of the webcast 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 the meeting. There will be an opportunity for stakeholders viewing the webcast to participate remotely in the meeting through a moderated conference bridge, including polling functionality. Access details for the meeting are subject to change. Please refer to NTIA's website, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security, for the most current information.

Dated: April 11, 2017.

Kathy D. Smith,
Chief Counsel,
National Telecommunications and Information Administration.
[FR Doc. 2017-07607 Filed: 4/13/2017 8:45 am; Publication Date: 4/14/2017]