Joint Comments on "Fostering the Advancement of the Internet of Things" Before the National Telecommunications and Information Administration

Docket No. 170105023–7023–01
Mar. 13, 2017

We the undersigned companies, civil society groups, and individuals submit these comments in response to the Department of Commerce's request for public comment on "Fostering the Advancement of the Internet of Things" (the "Green Paper").[1] We commend the Dept. of Commerce and the National Telecommunications and Information Administration's (NTIA) for their leadership on the Internet of Things (IoT) and cybersecurity, and for consistently soliciting the feedback of private sector experts.

We urge the Dept. of Commerce to actively encourage IoT providers and operators to develop and implement *coordinated vulnerability disclosure and handling processes*. Vulnerability disclosure and handling processes are formal internal mechanisms for receiving, assessing, and mitigating security vulnerabilities submitted in good faith by external sources, such as independent researchers, and communicating the outcome to the external vulnerability reporter and affected parties.

In its revisions to the IoT Green Paper, we recommend that the Dept. of Commerce consider

- More clearly articulating the benefit of adopting coordinated vulnerability disclosure and handling processes for IoT device and software providers, and
- Committing to continue working with industry, government bodies, and other stakeholders to promote coordinated voluntary adoption of vulnerability disclosure and handling processes.

IoT security strategies should include vulnerability disclosure and handling processes

The rapid growth of IoT devices are raising the number of uncorrected security vulnerabilities in consumer, business, and infrastructure environments. Left unchecked, some vulnerabilities can shift the danger from traditional online security to physical safety risks. Recognizing there is no perfect security and that all vulnerabilities cannot be completely eliminated from IoT devices pre-market, organizations must be prepared to discover, assess, and remediate cybersecurity flaws in their IoT devices throughout the device lifecycle. Yet the quantity, diversity, and complexity of connected devices and associated systems (such as apps or cloud offerings related to IoT) will prevent many IoT providers from catching all vulnerabilities without independent expertise or manpower. This may be especially true for vendors that are new entrants to the IoT ecosystem and have limited experience or resources for cybersecurity.

It is therefore increasingly important for technology providers and operators to establish coordinated vulnerability disclosure and handling processes. Having a vulnerability disclosure

[1] National Telecommunications and Information Administration, Notice, Request for public comments, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 82 FR 4313, Jan. 13, 2017, https://www.ntia.doc.gov/files/ntia/publications/fr_iot_notice_rfc_01132017.pdf.

and handling process in place – and communicating the existence and scope of that policy publicly – can help IoT providers and operators quickly address vulnerabilities disclosed to them by external sources, leading to mitigations that enhance the security, data privacy, and safety of IoT.[2] Such processes can also help protect researchers or accidental discoverers by providing them with a clear channel to communicate vulnerabilities to technology providers, reducing the risk of conflict or misunderstanding.

Such processes should be voluntary and need not actually incentivize searching for vulnerabilities (such as by offering bounties for bug submissions). Best practices, tactics, and standards for vulnerability disclosure and handling processes are available, but each vendor may tailor the process to meet its unique business model, technology, context, and resources.[3] Businesses and government agencies are increasingly implementing vulnerability disclosure and handling processes, but adoption of flexible and mature processes for handling unsolicited vulnerability reports is not yet the norm in the IoT industry.[4]

The Dept. of Commerce should continue promoting voluntary adoption of coordinated vulnerability disclosure and handling processes

The Dept. of Commerce should be commended for promoting discussion of vulnerability disclosure and handling processes through NTIA's multistakeholder effort, as well as its overall leadership on cybersecurity policy and coordination.[5] The multistakeholder effort has laid groundwork for greater understanding and collaboration between researchers and technology providers and operators.[6]

However, promoting broad IoT industry adoption and effective implementation will require a sustained effort. As written, the IoT Green Paper references coordinated disclosure and the

---

[2] *See, e.g.,* Matthew Finifter et al., An Empirical Study of Vulnerability Rewards Programs, 22nd Usenix Security Symposium, Aug. 14, 2013, https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf. " "We find that vulnerability reward programs (VRPs) appear to provide an economically efficient mechanism for finding vulnerabilities, with a reasonable cost/benefit trade-off[.] In particular, they appear to be 2-100 times more cost-effective than hiring expert security researchers to find vulnerabilities. We therefore recommend that more vendors consider using them to their (and their users') advantage."

[3] *See* ISO/IEC 30111:2013, Information Technology – Security Techniques – Vulnerability Handling, International Standards Organization, Nov. 1, 2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231. *See also* ISO/IEC 29147:2014, Information Technology – Security Techniques – Vulnerability Disclosure, International Standards Organization, Feb. 15, 2014, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170.

[4] *See* I Am The Cavalry, US Government Coordinated Disclosure, Dec. 2016, https://www.iamthecavalry.org/usgdisclosure. *See also* Sean Gallagher, *GM embraces white-hat hackers with public vulnerability disclosure program*, Ars Technica, Jan. 8, 2016, http://arstechnica.com/security/2016/01/gm-embraces-white-hats-with-public-vulnerability-disclosure-program.

[5] National Telecommunications and Information Administration, Multistakeholder Process: Cybersecurity Vulnerabilities, Dec. 15, 2016, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

[6] The NTIA process has also underscored the utility of vulnerability disclosure programs to both researchers and vendors – with stakeholders finding evidence that most researchers engage in coordinated disclosure when given the opportunity, resorting to public disclosure largely when communications with vendors did not meet expectations. NTIA Awareness and Adoption Group, Vulnerability Disclosure Attitudes and Actions, National Telecommunications and Information Administration, Dec. 15, 2016, https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf.

multistakeholder effort, but does not include content on the role of vulnerability disclosure and handling processes in the security strategies of IoT providers and operators.[7] The Green Paper also does not include an explicit commitment from the Department to promote adoption.

We recommend the Dept. of Commerce strengthen the IoT Green Paper by

- **More clearly articulating the benefit of adopting coordinated vulnerability disclosure and handling processes for IoT device and software providers.** This will make the Administration's IoT security policies more thorough and effective, and make the discussion of IoT security issues presented in the Green Paper more complete.[8]

- **Committing to continue working with the IoT industry, government bodies, and other stakeholders to promote voluntary adoption of coordinated vulnerability disclosure and handling processes.** Actively encouraging IoT providers and operators to adopt such processes is a key next step for the Department to take in fostering advancement of IoT security.[9] The Department should seek opportunities to incorporate vulnerability disclosure and handling processes in security guidance documents, such as the NIST Framework, that affect IoT and collaborate with other government agencies promoting vulnerability disclosure in IoT-related sectors.[10]

* * *

[7] National Telecommunications and Information Administration, Fostering the Advancement of the Internet of Things, Dept. of Commerce, Jan. 2017, pgs. 25, 41, https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

[8] National Telecommunications and Information Administration, Notice, Request for public comments, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 82 FR 4314, Jan. 13, 2017, https://www.ntia.doc.gov/files/ntia/publications/fr_iot_notice_rfc_01132017.pdf. "Is our discussion of IoT presented in the green paper regarding the challenges, benefits, and potential role of government accurate and/or complete? Are there issues that we missed, or that we need to reconsider?"

[9] National Telecommunications and Information Administration, Notice, Request for public comments, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 82 FR 4314, Jan. 13, 2017, https://www.ntia.doc.gov/files/ntia/publications/fr_iot_notice_rfc_01132017.pdf. “Are there specific tasks that the Department should engage in that are not covered by the approach? What should the next steps be for the Department in fostering the advancement of IoT?”

[10] *See, e.g.*, Federal Trade Commission, Federal Trade Commission Public Comment on NTIA Safety Working Group’s “Coordinated Vulnerability Disclosure ‘Early Stage’ Template”, Feb. 15, 2017, pg. 1, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-national-telecommunications-information-administration-regarding-safety-working/170215ntiacomment.pdf. *See also* Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff, Dec. 28, 2016, pg. 14, https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

We appreciate the opportunity to share our views. Thank you for your consideration.

Sincerely,

Rapid7
Access Now
Bugcrowd
Center for Democracy & Technology
Cybereason
Device Authority
Duo Security
Electronic Frontier Foundation
Global Cyber Alliance
Grimm
I Am The Cavalry
New America's Open Technology Institute
Niskanen Center
Online Trust Alliance
Security of Things Forum
WhiteScope

Brian Knopf, Senior Director of Security Research & IoT Architect, Neustar
Zach Lanier, Security researcher
Art Manion, CERT Coordination Center
Katie Moussouris, Founder and CEO, Luta Security, co-editor of ISO 29147 Vulnerability disclosure & ISO 30111 Vulnerability handling processes
Nicholas Percoco, Founder of THOTCON
Mark Stanislav, Security Researcher