Attn: Evelyn L. Remaley
National Telecommunications and
Information Administration (NTIA)
U.S. Department of Commerce
1401 Constitution Avenue NW., Room 4725,
Washington, DC 20230

February 12th, 2018

Comments of New America's Open Technology Institute:

A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Over the past decade the Internet of Things (IoT) industry has expanded dramatically, with the 2017 Ericsson Mobility Report predicting that there will be over 31 billion connected devices by the year 2020. This market has swelled far beyond what we could've predicted even ten years ago.[1] However, the proliferation of connected security cameras, baby monitors, digital video recorders, and refrigerators has also created 31 billion points for attack. New America's Open Technology Institute (OTI) welcomes the work NIST is doing to address these cybersecurity threats and appreciates the opportunity to comment on the recent draft paper "*A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*."[2] Our comments will focus specifically on the security threats posed by consumer edge devices.

Importance of Standardized Evaluation Metrics

When consumers walk into a store to choose which smartwatch they want to purchase they have very few things to go on: Is it a name brand I know? Do I like the color and style? What features does it provide? Nowhere on the box does it tell you anything about the digital security of the device inside. You carry these devices around with you wherever you go, but smartwatches, fitness monitors, or any of the other types of IoT devices collect vast amounts of personal data. When choosing to purchase and use these products consumers deserve to have much more information about the security and privacy of the device they are welcoming into their homes.

In reviewing NIST's most recent paper, OTI was pleased to see the conclusion that some broadly accepted, baseline security profiles for IoT devices are necessary to protect consumers.[3] Without these standardized security profiles, companies are able to sell products without meeting basic expectations or informing consumers about the security features of their products. The economic incentive to get new products to market as quickly as possible, and to limit the costs that additional digital protections might require, is a serious threat to user security. We were also pleased that NIST proposed that the federal

[1] "Ericson 2017 Mobility Report," November 2017, 14, available at https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-november-2017.pdf.
[2] "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," U.S. Department of Commerce, U.S. Department of Homeland Security, January 5, 2018, available at https://csrc.nist.gov/publications/detail/white-paper/2018/01/05/enhancing-resilience-against-botnets--report-to-the-president/draft.
[3] "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats," Goals and Actions, Goal 1, Action 1.1, p. 23.

government help accelerate the adoption of these standards by only purchasing IoT devices that meet these baseline security profiles.[4]

Industry-Driven Approaches Haven't Worked

However, OTI is concerned about the Report's recommendations about who should generate these security profiles. The Report identifies "industry" as the primary group who should be encouraged to develop IoT security standards. The Report encourages industry to engage with international standards organizations such as the Internet Engineering Task Force (IETF) and the International Organization for Standardization (ISO).[5] This is a good recommendation, but even here the Report leaves out consumer organizations and civil society.[6] This is a theme that repeats throughout the Report, and particularly in Goal 5.[7] Unfortunately, industry-led efforts to date and the nature of the market both lead to the conclusion that self-regulation is not likely to bring about solutions that effectively address the serious security issues we all face, even if done in consultation with civil society.

While self-regulation can be effective in some areas, too often we have seen such efforts fail. Often they simply trail off without producing anything concrete.[8] When they do produce an outcome, it is usually so watered down that it represents only the bare minimum of security features that most of the industry in question already meet. Civil society that does try to participate is routinely outnumbered and outspent.

This dynamic will only be exacerbated in the context of digital security because of the fundamental market failure in the area of device security. Many manufacturers are either unaware of their products' security lapses or simply don't care because there has never been a significant negative market impact as a result of poor security. Placing these organizations in charge of developing security standards would require convincing them of the need for those standards in the first place.

To create a credible baseline for security standards, the victims actually affected by failed security should be the stakeholders leading the conversation. Industry has to be involved and invested, of course, and suggestions made in good faith should be carefully considered, but consumer advocacy and civil society organizations should hold the reigns. The Report should be amended to reflect this preference.

There is already a security and privacy focused standard in development for NIST to point to. Called the Digital Standard, it is open source, and is being shepherded by a number of cybersecurity experts and civil society groups. Consumer Reports has also announced their intention to make use of it when rating "smart" devices. It could be the perfect platform for a consumer-focused security baseline.

What is the Digital Standard?

The Digital Standard is an open, collaborative effort to create a digital privacy and security standard which can help guide the future development of consumer software, digital platforms and services, and internet-connected products.[9] The Standard methodology is composed of 35 different "tests" that products can be measured against to see how they meet best practices. It also provides a model that companies can use to design and improve their products, ensuring that they are best in class on these security and privacy metrics.

[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] E.g., ibid., Actions 5.1 and 5.2.
[8] NTIA's own process on IOT security last met in November 2017 and does not appear to have released any final documents. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.
[9] "The Digital Standard," available at https://www.thedigitalstandard.org/.

Given OTI's concerns about NIST's suggestion of an industry-led regulation process, working with an already-existing framework could minimize some of those challenges. The Digital Standard was developed as a collaboration between civil society groups Disconnect,[10] Ranking Digital Rights,[11] the Cyber Independent Testing Lab,[12] and Aspiration,[13] as well as rating organization Consumer Reports.[14] This open-source process included contributions from cybersecurity experts who evaluated the tests and methodology from a technical perspective. This process gives it legitimacy as a framework that was developed with the interests of consumers, rather than companies, in mind. Manufacturers and developers also have an economic interest in conforming to the Digital Standard because of the influence rating organizations can have on their customers.

In fact, Consumer Reports is planning to incorporate digital security and privacy metrics into its existing ratings process. It has already used the Standard to rate Smart TVs, and has highlighted problems with certain Samsung and Roku products using this new evaluation system.[15] When products that were previously tested for screen resolution and sound clarity suddenly receive poor reviews because of security vulnerabilities, companies will have an incentive to get on board with this influential new evaluation system in a way that no industry-led regulation could achieve. When a ratings process has the ability to both give positive as well as negative reviews, it has more potential to move the market. This leads to a more effective outcome than with something like Energy Star – a self-certification metric which grades energy efficiency but fails to clearly highlight inefficient products.[16]

In this case, a framework like the Digital Standard could provide a tool to assist in the development of new products, allowing inexperienced companies to build new models with security features baked in. Companies without much experience in digital security, such as pre-digital appliance or household tools manufacturers who have only recently added connected capabilities to their products, may not have the skills or knowledge to implement the necessary protections for security and privacy.

The Standard is also still under development, with opportunities for stakeholders to contribute feedback and expertise into the testing metrics and process. Further engagement from industry and NIST, as well as civil society, can help create a more robust evaluation and development tool. Broad stakeholder participation would also help establish the Digital Standard as the best practice for IoT device security.

Conclusion

OTI appreciates the opportunity to comment on this version of the paper and hopes that this feedback may aid in the revisions process. A good set of base security standards is crucial to ensure the security of IoT products, and an existing, collaborative, and user-focused evaluation system is the best way of doing this. Given the the rapid expansion of the IoT market, and how many companies are entering the connected devices space, a tool like the Digital Standard is key to ensuring that these devices adequately protect the security and privacy of consumers.

For questions or additional information, please contact:

Ross Schulman, Senior Policy Technologist & Senior Counsel, New America's Open Technology Institute
ross@opentechinstitute.org

[10] "Disconnect: Who We Are," https://disconnect.me/about.
[11] "Ranking Digital Rights," https://rankingdigitalrights.org/.
[12] "Cyber ITL," https://cyber-itl.org/.
[13] "Aspiration," https://aspirationtech.org/.
[14] "Consumer Reports," https://www.consumerreports.org/cro/index.htm.
[15] "Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds," *Consumer Reports*, February 7, 2018, https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/.
[16] "ENERGY STAR Overview," https://www.energystar.gov/about.