Energy and Commerce Committee
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515
[redacted]

28 June 2018

Re: Supported Lifetimes Request for Information ("RFI")

Thank you for your work examining the use of internet-connected devices in the healthcare sector, specifically on the risks of "end of life" hardware and software issues.[1] We write today to highlight four important points for the Committee. While we respect prior submissions, we believe this additional information is necessary to clarify several issues that have been raised in response to this RFI. Additionally, we note that the points we raise today are not exclusive of the risks posed by poor device security and encourage the Committee to complete an in-depth review of the sector's security practices, including the impact on patients, prior to issuing any conclusions or recommendations.

1. Ineffective or unmaintained security of healthcare devices can have grave consequences.

   The HHS Health Care Industry Cybersecurity Task Force concluded in June 2017 that "Healthcare Cybersecurity is in Critical Condition," citing "epidemic" vulnerabilities in legacy healthcare equipment as foundational findings in its report.[2] While there are undoubtedly benefits associated with connectivity of healthcare devices, the long-term risks of poor security can be great. For example, in 2016 it was revealed that an implantable heart monitor had a vulnerability that allowed access to the devices through which a malicious actor could rapidly drain the battery, change the pacing, or issue shocks.[3] Luckily, the company behind the devices was able to issue a patch to remedy the vulnerability and no patient reported having been impacted. However, had no update been available, patients may have been left with a Hobson's choice of living with the risk of exploitation or undergoing surgery, with any associated financial or personal costs, to remove or replace the device. Capabilities meant to improve or save life, may also harm or end life; where failure impacts patient safety, a commensurate level of due care is warranted.

2. Manufacturers and suppliers are best situated to take responsibility for lifecycle planning.

[1] https://energycommerce house.gov/wp-content/uploads/2018/04/20180420Supported_Lifetimes_RFI.pdf.
[2] https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
[3] https://www fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843 htm.

Medical device support is a relay race across the stakeholder ecosystem, from component suppliers to manufacturers, to care delivery. No single stakeholder can be accountable for, or deliver all legs of this race, and others have a role to play, such as regulators, insurers, caregivers, and patients. In fact, device operators or beneficiaries often don't possess or have access to the technical knowledge necessary to fully measure and understand the full scope of potential vulnerabilities for a specific internet-connected product or service. However, manufacturers who bring products to market are in the best position to understand and balance safety, security, and effectiveness throughout the useful lifetime of the device.

Ownership and accountability does not resolve several outstanding tensions, however, that Congress must keep in mind. The period that a healthcare device maintains its practical utility often exceeds the shelf life intended by the manufacturer(s) of the device and / or of its component pieces. This mismatch is particularly hard to plan for when devices include open source components maintained by volunteers for which long term support is hard to predict. However, manufacturers' reputations are dependent on caregivers accepting support, including timely updating and patching, and proper planning and communication can mitigate some of the more dire consequences for when that doesn't happen.

In response, and in concert with others in the ecosystem, manufacturers should:

- build in capabilities to empower continued safe and effective operation;
- have a plan for obsolescence;
- communicate clearly and provide support for the planned lifetime;
- provide guidance for continued safe and effective care delivery, after the planned lifetime of the device;[4] and
- ensure supported lifetime of components, including those who rely on open source projects, matches planned lifetime of the device.[5]

3. Buyers, patients, and care providers must be equipped to make informed choices.

Underinvestment in safety, security, and privacy of healthcare devices can put national security, the national economy, and public safety at risk. To correct for this, it's important that caregivers can distinguish among similar products and understand costs, responsibilities, and risks. It isn't enough to assert, as one industry group did in response to this RFI, that

---

[4] *See, e.g.*, The Charter of Trust (Signed by over a dozen companies, including medical device makers and insurers), *available at* https://www.siemens.com/global/en/home/company/topic-areas/digitalization/cybersecurity html ("Companies must offer updates, upgrades, and patches throughout a reasonable lifecycle for their products...").

[5] *See, e.g.*, https://arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-finally-agree-to-fund-openssl.

"maintaining device and information security is a shared responsibility of the manufacturers and suppliers of connected devices and services, as well as the providers that use them."[6]

Instead, to fully realize benefits of internet-connected healthcare devices, and mitigate serious risks, it is incumbent that providers and manufacturers commit to providing buyers, patients, and caregivers with the necessary information and mechanisms to facilitate informed decisions and actions on product security. In practice,this means that manufacturers should precisely communicate the anticipated period through which security updates and patches will be provided, adopt processes to receive and act on relevant vulnerability reports, providing a software bill of materials,[7] and inform caregivers on the availability of rebates or other incentives that will be provided for upgrading software or equipment at the end of life, among other things.

4. Externalities cannot be solved with information parity and call for other options.

   While the market may be able to incentivize positive security practices in some instances, recent events have demonstrated areas where these forces do not reach, or may even exacerbate the problem.[8] The Mirai botnet, which caused broad service outages among several US Internet companies, takes advantage of characteristics similar to those found in medical devices - namely, hard coded default credentials.[9] In cases like Mirai where policy failures and externalities persist, minimum hygiene standards can bridge the gap. It would be useful to evaluate broadly how minimum standards or accountability for harm can address cybersecurity market externalities and market failures.[10]

The disconnect between the security support cycle and practical lifecycle of connected healthcare devices cannot be the basis for disregarding or minimizing the risks outdated devices pose to healthcare recipients. An appropriate response will require an understanding the extent of the risks and coordination to develop processes to minimize those risks.

---

[6] http://www.supplychainassociation.org/wp-content/uploads/2018/05/HSCA-Final-Supported-Lifetimes-Comments-to-House-EC-05.31.18.pdf.

[7] https://energycommerce.house.gov/news/press-release/walden-asks-hhs-convene-sector-wide-effort-develop-software-bill-materials-health-care-technologies/

[8] From p. 17, "Market incentives appear to exacerbate the problem. Product developers prioritize time to market and innovative functionality over security and resilience. Security features are not easily understood or communicated to the consumer, which makes it difficult to generate demand." https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf

[9] https://umbrella.cisco.com/blog/2017/01/05/future-assaulting-internet-mirai/.

[10] https://www nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

We look forward to working with the House Committee on Energy and Commerce Committee and industry actors to find and promote solutions that ensure medical technology provides not only the medical care but security expected by patients.

Thank you,

Access Now
Consumers Union
New America's Open Technology Institute

L Jean Camp, Indiana University
Jonathan Cran, Kenna Security (Head of Research)
Anna Lysyanskaya, Brown University
Beau Woods, I Am the Calvary (Cyber Safety Volunteer)