AdvaMed
Advanced Medical Technology Association

701 Pennsylvania Avenue, NW
Suite 800
Washington, D.C. 20004–2654
Tel: 202 783 8700
Fax: 202 783 8750
www.AdvaMed.org

June 12, 2018

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

Re: Supported Lifetimes Request for Information

Dear Chairman Walden and Ranking Member Pallone:

The Advanced Medical Technology Association ("AdvaMed") appreciates the opportunity to provide input to the U.S. House of Representative's Committee on Energy and Commerce ("Committee") in response to its Supported Lifetimes Request for Information ("RFI").[1] AdvaMed represents manufacturers of digital health technologies, medical devices, and diagnostic products that are transforming health care through earlier disease detection, less invasive procedures, and more effective treatment. Our members range from the smallest to the largest medical technology innovators and companies.

I. The Medical Technology Industry's Cybersecurity Efforts and Requirements

Patient safety is the number one priority for the medical technology industry, and medical device manufacturers take seriously the need to continuously assess the security of their devices in a world where technology constantly evolves. Medical device manufacturers make concerted efforts to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data. During the postmarket phase, manufacturers implement proactive measures to manage medical device cybersecurity, including, but not limited to, routine device cyber maintenance, assessing postmarket information, employing risk-based approaches to characterizing vulnerabilities, and timely implementation of necessary actions.

A. AdvaMed Cybersecurity Principles

AdvaMed's Board of Directors adopted foundational medical device cybersecurity principles[2] that, in addition to being received positively by many government agencies and other stakeholders, serve as a commitment by our industry to ensuring medical device cybersecurity threats are addressed in a meaningful way. Indeed, the first of the five

[1] https://energycommerce.house.gov/wp-content/uploads/2018/04/20180420Supported_Lifetimes_RFI.pdf.

[2] AdvaMed Medical Device Cybersecurity Foundational Principles (Nov. 2016), *available at* https://www.advamed.org/sites/default/files/resource/advamed_medical_device_cybersecurity_principles_final.pdf.

principles—medical device development and security risk management—states that a firm's cybersecurity risk management program should address cybersecurity from medical device conception through disposal.

The second of our principles states that system-level security is a shared responsibility among all stakeholders within the larger system. Stakeholders include medical technology companies, hospitals, physicians, IT professionals, providers, regulators and patients. The RFI highlights this point as medical devices are often connected to a third-party network, such as in a patient's home or in a hospital, which may provide various means to access and direct the medical device outside of the manufacturer's control. Today, manufacturers and health care institutions actively participate in numerous groups and organizations that bring together the healthcare industry to address cybersecurity. One such organization is the Health and Healthcare Sector Cybersecurity Coordinating Council, which has a task force dedicated to examining issues concerning medical device cybersecurity.

In our principles, we also state that the development of consensus standards and regulations should be a collaborative effort between regulators, medical device manufacturers, independent security experts, academics, and health care delivery organizations. We believe these standards need to be applied consistently across the entire health care industry.

In support of this principle, the medical device industry actively participates in the development of cybersecurity consensus standards, including the following that are now finalized:

1. AAMI TIR57:2016, *Principles for medical device security—Risk management* (FDA Recognition Number 13-83).

2. IEC 80001-1 series including ANSI/AAMI/IEC TIR 80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices ─ Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls* (FDA Recognition Number 13-43).

3. HIMSS/NEMA HN 1-2013, *Manufacturer Disclosure Statement for Medical Device Security*.

B. Regulatory Requirements

The medical device industry's chief regulator, the U.S. Food and Drug Administration ("FDA"), administers comprehensive regulations and implementing guidance that prescribe risk management requirements that medical technology manufacturers must comply with, and for which they would face severe penalties for failing to follow. FDA's cybersecurity requirements address cybersecurity in both pre-[3] and post-market[4] environments. FDA also has hosted three cybersecurity workshops, and the medical device industry actively participated in them.[5]

More recently, FDA proposed taking further steps to enhance medical device cybersecurity through the release of its Medical Device Safety Action Plan.[6] Among other items, the Action Plan proposes to: (1) Require medical device manufacturers to submit as part of their presubmission material a software bill of material and information concerning the ability to update and patch the device's security; and (2) require manufacturers to institute coordinated disclosure policies. Our industry strongly supports the use of coordinated vulnerability disclosure (it is the third of our cybersecurity principles), as the process informs stakeholders, including healthcare IT personnel, of current risks and appropriate mitigating controls. Coordinated vulnerability disclosure processes have been adopted by all large medical device manufacturers, and most manufacturers maintain a web page to support intake of vulnerabilities from researchers and other sources.

II. AdvaMed Comments Concerning Statements Made In the RFI

While we appreciate the context provided in the RFI, we believe several statements require further clarification. First, while the RFI suggests a misalignment between advancements in medical device technology and overall technology, it does not directly acknowledge that medical devices cannot support updates beyond the useful life of the underlying technology, which for common off-the-shelf components can be as short as 3-4 years. Once a technology is depreciated (*e.g.*, 32-bit processors, encryption algorithms, total system storage and memory, and other hardware limitations), updates are either no longer available or not possible. Manufacturers and health care delivery organizations typically implement defense-in-depth controls to mitigate risks presented by legacy technologies; however, these technologies simply cannot be supported in perpetuity.

We do not believe the following statement in the RFI is accurate: "The WannaCry outbreak

[3] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff (Oct. 2, 2014), *available at* https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

[4] Postmarket Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff (Dec. 28, 2016), available at https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

[5] Public Workshop – Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis (May 18-19, 2017); Moving Forward: Collaborative Approaches to Medical Device Cybersecurity, Public Workshop, Request for Comments (Jan. 20-21, 2016); Public Workshop – Collaborative Approaches for Medical Device and Healthcare Cybersecurity (Oct. 21-22, 2014).

[6] Medical Device Safety Action Plan (April 17, 2018), *available at* https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf.

occurred primarily because of one protocol embedded within dozens of unique medical technologies." The WannaCry outbreak impacted all critical infrastructure sectors and was not unique to the Healthcare and Public Health Sector. As noted in ICS-CERT Alert TA17-132A, "[a]ccording to numerous open-source reports, a widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in over 150 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as 27 different languages."[7]

We also believe the following statement significantly underestimates the cost of remediating a single vulnerability: "Though hard data about the exact costs are difficult to determine, one cybersecurity professional estimated that fixing a single vulnerability may cost an organization anywhere from $400 to $4,000." For a typical vulnerability, the specified range underestimates costs by an order of magnitude due to labor costs associated with development, verification and validation, risk management file revision, customer communication, and regulatory requirements. Additional costs on the user/owner side could also be incurred to apply the solution.

Lastly, we agree with the statement that "[p]olicies that would require manufacturers to support legacy technologies indefinitely would therefore likely have significant impacts on their ability to provide new and innovative technologies, as their resources would necessarily have to be spent maintaining their legacy products." AdvaMed agrees that adoption of policies to support legacy technologies indefinitely would slow the development of new and innovative medical technologies, and may have a direct impact on the financial viability of smaller innovative manufacturers.

III. Challenges, Opportunities, Considerations, and Suggestions

The 2017 Health Care Industry Cybersecurity Task Force Report[8] ("Report") identifies four recommendations with respect to securing legacy medical devices and health IT systems. The recommendations, which our industry supports, are:

- **Action Item 2.1.1:** Health delivery organizations must: (1) inventory their clinical environments and document unsupported operating systems, devices, and EHR systems; (2) replace or upgrade systems with supported alternatives that have superior security controls where possible; (3) develop and document retirement timelines where devices cannot yet be replaced; and (4) leverage segmentation, isolation, hardening, and other compensating risk reduction strategies for the remainder of their use.

[7] Alert TA17-132A, Indicators Associated With WannaCry Ransomware (May 12, 2017), *available at* https://www.us-cert.gov/ncas/alerts/TA17-132A.

[8] Health Care Industry Cybersecurity Task Force, Report on Improving Cybersecurity in the Health Care Industry (June 2017), *available at* https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

- **Action Item 2.1.2:** Health care sector accreditation organizations (*e.g.*, Joint Commission, and Centers for Medicare & Medicaid Services (CMS)) must: (1) consider incentives, requirements, and/or guidelines for reporting and/or use of unsupported system and mitigation strategies; and (2) develop aggressive timelines for conformance.

- **Action Item 2.1.3:** For devices that still receive some support from the device manufacturer and/or application vendor, these organizations must make real-time updates and patches (*e.g.*, to the operating system), as well as make compensating controls available to end users. Organizations should also have a policy/plan in place to be able to receive and implement available updates.

- **Action Item 2.1.4:** Government and industry should develop incentive recommendations to phase-out legacy and insecure health care technologies (e.g., incentive models like Cash for Clunkers, Montreal Protocol, and Federal IT Modernization Fund). As a part of looking at incentives, government and industry should create partnerships/alliances to establish roadmaps for joint enhancement of cybersecurity interoperability and maturity through better procurement processes.[9]

Furthermore, given that technology is constantly changing and innovative devices quickly become obsolete as new discoveries are introduced, we believe device manufacturers should proactively communicate "end of support" dates to ensure that customers possess sufficient information to plan transition periods for legacy technologies. AAMI is developing a new Technical Information Report, TIR97, *Principles for medical device security — Postmarket risk management for device manufacturers*. The current draft of this document defines "end of support" and addresses relevant issues in Clause 6, Retirement/obsolescence.

* * *

AdvaMed would like to thank the Committee for its consideration of this letter and looks forward to continuing to work together on these important issues. Please do not hesitate to contact me at 202-434-7224 or zrothstein@advamed.org if you have any questions.

Respectfully submitted,

/s/

Zachary A. Rothstein, Esq.
Associate Vice President
Technology and Regulatory Affairs

[9] *Id.* at pp. 28-29.