GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

November 16, 2017

The Honorable Eric D. Hargan
Acting Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Acting Secretary Hargan:

As evidenced by events in the past several years, cyber threats to the health care sector are becoming more numerous, more frequent, and more severe. The sector has proved to be increasingly vulnerable to both targeted attacks, such as the theft of information, and indiscriminate exploits such as the WannaCry and NotPetya malware.[1] In addition, security researchers and others have exposed a number of vulnerabilities in widely used medical technologies.[2] While the sector's susceptibility to cyber threats has many causes, a significant and frequent source of risk is due to the fact that many of the technologies leveraged by health care stakeholders are, in essence, "black boxes." Stakeholders do not know, and often have no way of knowing, exactly what software or hardware exist within the technologies on which they rely to provide vital medical care. This lack of visibility directly affects the ability of these stakeholders to assess their levels of risk and adjust their strategies appropriately.

---

[1] Lily Hay Newman, *The Ransomware Meltdown Experts Warned About is Here*, WIRED, Mar. 12, 2017, https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/; Lily Hay Newman, *A Scary New Ransomware Outbreak Uses WannaCry's Old Tricks*, WIRED, June 27, 2017, https://www.wired.com/story/petya-ransomware-outbreak-eternal-blue/; Dan Munro, *Data Breaches in Healthcare Totaled Over 112 Million Records in 2015*, FORBES, Dec. 31, 2015, https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#56e1a0c27b07.

[2] Sean Gallagher, *Two more healthcare networks caught up in outbreak of hospital ransomware,* ARS TECHNICA, Mar. 29, 2016, https://arstechnica.com/information-technology/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware/; *Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication*, FDA, Jul. 31, 2015, https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm456815.htm; *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication*, FDA, Jan. 9, 2017, https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm; *Johnson & Johnson Warns Patients of an Insulin Pump Cyber Bug*, REUTERS, Oct. 4, 2016, http://fortune.com/2016/10/04/johnson-johnson-insulin-pump-cyber-bug/.

Recent events have highlighted the increasing – and potentially serious repercussions – of organizations lacking visibility or awareness about the products and services they leverage on a daily basis. For example, in the WannaCry and NotPetya outbreaks, both strains of malware relied on a vulnerability within a widely used protocol known as SMBv1.[3] During these outbreaks, a critical part of stakeholders' response efforts was to identify which technologies within their networks leveraged SMBv1, and then to take appropriate steps to "quarantine" and otherwise protect these technologies from infection. However, because information detailing which pieces of technology contain which protocols is often severely lacking or altogether unavailable, stakeholders were forced to take less targeted, and thus less effective, remediation steps, or to contact the manufacturers individually to try and obtain the missing information. For health care organizations that may have thousands of technologies in use, this slow, manual process actively harms their ability to respond to cybersecurity emergencies and thus their ability to protect patients.

While WannaCry and NotPetya represent two of the most illustrative cases of the types of issues created by the "black box" nature of most modern medical technologies, other instructive examples exist. For example, in 2016, researchers warned of a vulnerability in the popular software package "JBoss" leveraged by a ransomware variant known as "Samsam." Several hospitals experienced disruptions due to Samsam and the JBoss vulnerability.[4] In 2015, a security researcher discovered several medical devices that relied on a protocol known as Telnet, the use of which could have allowed unauthorized users to send commands to the device.[5] Telnet has been considered insecure and thus use of the protocol discouraged, for many years.[6] Similarly, other medical devices were found to use an insecure protocol known as the "File Transfer Protocol" or "FTP."[7] Like Telnet, cybersecurity best practices recommend against the use of FTP.[8] Still other medical devices have been found to use operating systems such as Windows Server 2003 or Windows XP, which have been considered legacy operating systems for several years, and contain many known vulnerabilities.[9]

The existence of insecure or outdated protocols and operating systems within medical technologies is a reality of modern medicine. At the same time, however, this leaves health care

---

[3] *Microsoft Security Bulletin MS17-010 – Critical*, MICROSOFT TECHNET, Mar. 14, 2017, https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.
[4] Gallagher, *supra.*
[5] *Advisory (ISCA-15-125-01B) Hospira LifeCare PCA Infusion System Vulnerabilities (Update B)*, ICS-CERT, June 10, 2015, https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B.
[6] Wayne Jansen, Karen Scarfone , & Miles Tracy, *Guide to General Server Security*, NATIONAL INSTITUTE OF STANARDS AND TECHNOLOGY, July 2008, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf ("[D]o not use less secure protocols (e.g., telnet, FTP, NFS, HTTP) unless absolutely required . . . ").
[7] *Advisory (ICSMA-17-250-02) Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities*, ICS-CERT, Sept. 7, 2017, https://ics-cert.us-cert.gov/advisories/ICSMA-17-250-02.
[8] Jansen, *supra.*
[9] *Advisory (ICSMA-16-089-01) – CareFusion Pyxis SupplyStation System Vulnerabilities*, ICS-CERT, Mar. 23, 2017, https://ics-cert.us-cert.gov/advisories/ICSMA-16-089-01; *Microsoft Windows Xp: Security Vulnerabilities*, CVE DETAILS, https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-739/Microsoft-Windows-Xp.html; *Microsoft Windows Server 2003: Security Vulnerabilities*, CVE DETAILS, https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-7108/Microsoft-Windows-Server-2003.html.

organizations vulnerable to increasingly sophisticated and rapidly evolving cyber threats.[10] While visibility into the types of software and hardware within technologies is not a panacea or silver bullet for complex cyber threats, it is an important component of elevating the security posture of health care organizations. After all, an organization cannot protect what it does not know it has.

This challenge was recently examined by the statutorily established Health Care Industry Cybersecurity Task Force (Task Force). In their final report on Improving Cybersecurity in the Health Care Industry, the Task Force recommended a "bill of materials" (BOM) as a potential solution to this problem. As envisioned in the report, a BOM would exist for each piece of medical technology and would "describe [the technology's] components (e.g., equipment, software, open source, materials), as well as any known risks associated with those components."[11] The Task Force explained their recommendation, stating:

> Having a "bill of materials" is key for organizations to manage their assets because they must first understand what they have on their systems before determining whether these technologies are impacted by a given threat or vulnerability. Moreover, this transparency enables health care providers to assess the risk of medical devices on their networks, confirm components are assessed against the same cybersecurity baseline requirements as the medical device, and implement mitigation strategies when patches are not available.[12]

The Task Force's report, post-outbreak analyses of WannaCry and NotPetya, and Committee staff work on health care issues all demonstrate the risks presented by the continued prevalence of insecure and legacy components in health care technologies. This situation is untenable and elevates the need to explore the Task Force's recommendation on the creation and deployment of BOMs. While the implementation and use of BOMs will not completely protect the health care sector from cyber threats, it is an important, common-sense step towards improving the cybersecurity of the sector overall.

As such, we write today to request that the Department of Health and Human Services convene a sector-wide effort to develop a plan of action for creating, deploying, and leveraging BOMs for health care technologies. This will require an open and collaborative process to ensure that all interested stakeholders have an opportunity to contribute to this discussion in the interest of achieving the strongest and most effective solution.

We understand that this request will require significant coordination and effort among several diverse stakeholders, and we therefore request that you provide us with a plan of action for convening the sector no later than December 15, 2017. In addition, we request that by

---

[10] *See supra* note 1.
[11] *Report on Improving Cybersecurity in the Health Care Industry*, HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE, June 2017, https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf.
[12] *Id.*

December 22, 2017, you make your staff available to provide a briefing to the Committee on this work.

We appreciate your assistance with these requests. If you should have any questions, please contact Jessica Wilkerson or John Ohly of the Committee staff at (202) 225-2927.

Sincerely,

Greg Walden
Chairman

cc: The Honorable Frank Pallone, Jr., Ranking Member

The Honorable Diana DeGette, Ranking Member
Subcommittee on Oversight and Investigations