BRETT GUTHRIE, KENTUCKY
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED NINETEENTH 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) 225-3641
Minority (202) 225-2927

March 30, 2025

MEMORANDUM

TO: Members of the Subcommittee on Oversight and Investigations
FROM: Committee on Energy and Commerce Majority Staff
RE: Subcommittee on Oversight and Investigations Hearing on April 1, 2025

I. INTRODUCTION

The Subcommittee on Oversight and Investigations will hold a hearing on Tuesday, April 1, 2025, at 10:30 a.m. (ET), in 2322 Rayburn House Office Building. The hearing is entitled, "Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices."

II. WITNESSES

- **Christian Dameff, MD, MS, FACEP,** Emergency Physician and Co-Director, Center for Healthcare Cybersecurity, University of California San Diego Health;
- **Greg Garcia,** Executive Director, Health Sector Coordinating Council Cybersecurity Working Group;
- **Erik Decker,** Vice President and Chief Information Security Officer, Intermountain Healthcare;
- **Michelle Jump,** Chief Executive Officer, MedSec; and
- **Kevin Fu, PhD,** Professor, Department of Electrical and Computer Engineering, Khoury College of Computer Sciences, Department of Bioengineering, Kostas Research Institute (KRI) for Homeland Security, Northeastern University.

III. BACKGROUND

A. Legacy Medical Devices

Legacy medical devices are medical devices that "cannot be reasonably protected against current cybersecurity threats."[1] The term "legacy medical device" is applicable to medical devices that were produced under old medical device requirements and do not have the same cybersecurity considerations incorporated into modern medical device designs today.[2] The term also applies to newer devices that "cannot be reasonably protected against current cybersecurity threats."[3]

There is a broad range of medical devices that could be vulnerable to cyberattacks including patient monitors, infusion pumps, pacemakers, insulin pumps, intracardiac defibrillators, mobile cardiac telemetry, pacemakers, intrathecal pain pumps, and imaging devices.[4] While medical device hardware can remain functional for 10 to 30 years, the software life cycles of these devices are often much shorter. [5] The software cycle is specified by the device manufacturer, and ranges "from a couple of months to maximum life expectancy per device allowing cyber threat actors time to discover and exploit vulnerabilities."[6]

Cybersecurity measures that were effective at purchase may no longer adequately protect against present threats.[7] This is due to the extended lifespans of medical devices—many of which are network-connected—and inconsistencies between medical device manufacturers (MDM) and health care delivery organizations (HDO) regarding support and replacement practices for these devices. For instance, an MRI machine that has been in use for decades, and continues to function well in a clinical setting, may no longer have cybersecurity support available due to its age.[8] This creates a significant challenge in maintaining the security of these devices over their extended lifetimes.[9]

---

[1] Medical Device Cybersecurity Working Group, *Principles and Practices of Cybersecurity for Legacy Medical Devices (IMDRF/Cyber WG/N70Final:2023)*, INTERNATIONAL MEDICAL DEVICE REGULATORS FORUM (Apr. 11, 2023), at 8, https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices.
[2] *Id.*
[3] *Id.* at 5.
[4] *Id.*; Federal Bureau of Investigation (FBI) Cyber Division, Private Industry Notification, *Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities*, PIN Number 20220912-001, FBI PRIVATE INDUSTRY NOTIFICATION (Sept. 12, 2022), https://www.ic3.gov/CSA/2022/220912.pdf; *see also*, Greg Slabodkin, *Legacy medical devices, growing hacker threats create perfect storm of cybersecurity risks,* MEDTECH DIVE (June 22, 2021), https://www.medtechdive.com/news/legacy-medical-devices-growing-hacker-threats-create-medtech-cyber-risks/602157/; Theresa Defino, *Securing Problematic 'Legacy' Devices: Be Part of Procurement, Push for Info*, JD SUPRA (Mar. 14, 2022), https://www.jdsupra.com/legalnews/securing-problematic-legacy-devices-be-3441853/.
[5] FBI, *supra* note 4.
[6] *Id.*
[7] MITRE, *Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks,* (Nov. 2023), at 1, https://www mitre.org/sites/default/files/2023-11/PR-23-3695-Managing-Legacy-Medical-Device%20Cybersecurity-Risks.pdf.
[8] Government Accountability Office (GAO), *Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination*, GAO-24-106683 (Dec. 2023), at 9, https://www.gao.gov/assets/gao-24-106683.pdf.
[9] *Id.*

According to a research report cited in a private industry notification sent by the Cyber Division of the Federal Bureau of Investigation (FBI), "53 [percent] of connected medical devices and other internet of things devices (IoT) in hospitals had known critical vulnerabilities."[10] Although exact figures on usage of legacy medical devices in the U.S. health care system are not publicly known, this research report suggests the potentially significant scale of the legacy medical device problem.[11]

B. Legacy Medical Device Vulnerabilities and Risks

As noted in a March 2023 Healthcare and Public Health Sector Coordinating Councils (HSCC) report, "cyber threats to the healthcare sector are a well-documented reality of modern healthcare delivery."[12] Despite the devices' vulnerability to cyber threats, "an attacker's goal is rarely to hack into a singular device like a pacemaker or an insulin pump and take control."[13] A medical device, however, "can be used as an entry point to get onto a larger target, such as a hospital's network."[14] Below are some examples of medical devices where vulnerabilities have been identified.

On January 30, 2025, the Cybersecurity and Infrastructure Security Agency (CISA) released an alert along with a notification from the Food and Drug Administration (FDA) suggesting that a patient monitor, Contec CMS8000, contained a backdoor that could communicate with a Chinese IP address.[15] A backdoor is defined as "a way to access a computer system or encrypted data that bypasses the system's customary security mechanisms."[16] The equipment made by Contec Medical Systems in China, was configured to connect to an IP address belonging to the China Education and Research Network at Tsinghua University in Beijing, which had no apparent connection with the manufacturer.[17] The university was not named in the CISA alert, nor the FDA notice.

---

[10] FBI, *supra* note 4.
[11] MITRE, *supra* note 7, at 6.
[12] Healthcare and Public Health Sector Coordinating Councils (HSCC), *Health Industry Cybersecurity: Managing Legacy Technology Security (HIC-MaLTS)*, (Mar. 2023), at 4, https://healthsectorcouncil.org/wp-content/uploads/2023/03/Health-Industry-Cybersecurity-Managing-Legacy-Technology-Security-HIC-MaLTS.pdf.
[13] Ricky Zipp, *As cyberattacks on healthcare persist, can the FDA's new device regs hold up?,* MEDTECH DIVE (Apr. 3, 2024), https://www.medtechdive.com/news/medical-device-cybersecurity-risks-future/712112/.
[14] *Id.*
[15] Cybersecurity and Infrastructure Security Agency (CISA), CISA Releases Fact Sheet Detailing Embedded Backdoor Function of Contec CMS8000 Firmware (January 30, 2025), https://www.cisa.gov/news-events/alerts/2025/01/30/cisa-releases-fact-sheet-detailing-embedded-backdoor-function-contec-cms8000-firmware; *See also* Cybersecurity and Infrastructure Security Agency (CISA), *Contec Health CMS8000 Patient Monitor (Update A),* ICS MEDICAL ADVISORY (Feb. 25, 2025), https://www.cisa.gov/news-events/ics-medical-advisories/icsma-25-030-01; Food and Drug Administration (FDA), *Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication* (Jan. 30, 2025), https://www fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-patient-monitors-contec-and-epsimed-fda-safety-communication; *see also* CISA, *Contec CM8000 Contains a Backdoor,* FACT SHEET (Feb. 13, 2025), https://www.cisa.gov/resources-tools/resources/contec-cms8000-contains-backdoor.
[16] Ben Lutkevich & Brien Posey, *Definition: Backdoor (Computing),* TECHTARGET (Jan. 2023), https://www.techtarget.com/searchsecurity/definition/back-door.
[17] Billy Rios, *Billy Rios' Post,* LINKEDIN (Feb. 11, 2025), https://www.linkedin.com/posts/billyrios_i-find-it-hilarious-that-cisa-and-claroty-activity-7294800043088261120-IU0U; *see* Michael Kan, *Chinese-made Patient Monitor Contains a Secret Backdoor*, PC MAGAZINE (Jan. 31, 2025), https://www.pcmag.com/news/chinese-made-patient-monitor-contains-a-secret-backdoor.

According to CISA, the backdoor enables the IP address at the university to remotely download and execute unverified files on the patient monitor.[18] In addition, the backdoor can automatically send patient data to the IP address.[19] There are two schools of thought regarding the backdoor found on the monitors: (1) the patient monitor is a low-quality product with inadequate cybersecurity controls; or (2) the backdoor represents a deliberate Chinese attempt to undermine U.S. digital infrastructure. An investigation by a cybersecurity firm concluded that it was most likely not a hidden backdoor, but instead a vulnerable design that introduces great risk to patient monitor users and hospital networks.[20]

The patient monitor device was cleared by FDA in 2011, years before FDA began robust reviews of cybersecurity in medical devices as part of the premarket evaluation of safety and efficacy from 2019 to 2020, or before 2022 federal law required such.[21] CISA and FDA, however, referred to the issue with the patient monitor as a "backdoor," signaling heightened concerns over the cybersecurity and vulnerabilities of the devices.[22] Moreover, a cybersecurity firm noted that in 2018, hackers working from Tsinghua University—which is known as "China's MIT"—targeted U.S. energy companies, communications companies, and the Alaskan state government.[23] A representative of the same cybersecurity firm said it was unclear whether the targeted systems were compromised, but noted that "the highly focused, extensive and peculiar scanning activity" indicated a "serious interest" in hacking the targets.[24]

Neither CISA nor FDA have an indication of direct harm from these devices, but several possibilities of harm exist.[25] For example, because the affected devices are capable of running third-party code, they could be exploited by malicious actors, and malicious code could be used to disable monitoring or corrupt data.[26] This could lead providers to miss health issues or provide incorrect treatment.[27] Given these risks, it is concerning that the backdoor issue on this patient monitor was overlooked for more than 13 years.

---

[18] *Id.*
[19] *Id.* (The backdoor was described by CISA as a "reverse backdoor." A reverse backdoor is "[a] method that allows attackers to connect to remote computers through firewalls. It is used when conventional methods are not successful. Reverse Shell enables cybercriminals to execute arbitrary commands on operating systems and gain full control over the target computers. The underlying logic behind the use of Reverse Shell is to connect to a controlled computer and request a shell session during a typical remote shell setup. If direct access to the remote host is not possible, Reverse Shell comes into play. It connects to a listening network host from the outside and creates a shell session, providing attackers access to the target computer's operating system." (SwordSec, *Reverse Shell and Backdoor: What Are the Differences?,* BLOG (Aug. 2, 2023), https://swordsec.com/reverse-shell-and-backdoor/.))
[20] Team82, *Do the CONTEC CMS8000 Patient Monitors Contain a Chinese Backdoor? The Reality is More Complicated*..., CLAROTY TEAM82 (Feb. 2, 2025), https://claroty.com/team82/research/are-contec-cms8000-patient-monitors-infected-with-a-chinese-backdoor-the-reality-is-more-complicated.
[21] FDA, *510(k) Premarket Notification: K101692*, *Summary,* FDA MEDICAL DEVICES DATABASE, https://www.accessdata fda.gov/cdrh_docs/pdf10/K101692.pdf.
[22] CISA & FDA s*upra* note 15.
[23] Christopher Bing & Jack Stubbs, *Chinese hackers targeted U.S. firms, government after trade mission: researchers,* REUTERS (Aug. 16, 2018), https://www reuters.com/article/world/chinese-hackers-targeted-us-firms-government-after-trade-mission-researchers-idUSKBN1L11DX/.
[24] *Id.*
[25] Michael Lieberman, *Alarms Raised by Critical Reverse Backdoor Vulnerability in Medical Devices*, KUSARI (Feb. 3, 2025), https://www.kusari.dev/blog/reverse-backdoor-medical-devices.
[26] *Id.*
[27] *Id.*

While identification of the patient monitor vulnerability is a more recent example, cybersecurity vulnerabilities have been identified across a range of medical devices commonly used in clinical care.[28] For example, vulnerabilities have previously been identified in infusion pumps, insulin pumps, pneumatic tube systems, and medical imaging devices.[29] MDMs and HDOs typically work to mitigate vulnerabilities as soon as they are known; however, these examples illustrate the persistent cybersecurity challenges facing legacy and connected medical technologies.[30]

One of the concerns regarding legacy medical device cybersecurity vulnerabilities, is the risk posed to patient safety. These risks have the potential to negatively impact clinical outcomes. Specifically, if a medical device's vulnerability is exploited, the ability for a device to help monitor, diagnose, or treat a patient can be compromised. For example, "[t]here have been cases where insulin pumps have been hacked, and this security flaw meant that the hackers could raise dose limits without the patient's knowledge or consent."[31]

In addition to patient safety risks, cybersecurity vulnerabilities also pose broader risks to public health security. The health care and public health sector is one of sixteen industry sectors that has been designated as "critical infrastructure" in the U.S., and it has faced an increasing number of damaging cyber-attacks, making it vital to consider cybersecurity vulnerabilities in the health care space through a security lens.[32] Such vulnerabilities can create risks to and compromise medical device functions, patient information and medical data, as well as hospital systems and their data. For example, the ransomware group ALPHV (BlackCat) breached Change Healthcare in 2023, exposing sensitive patient data, disrupting claims, pharmacy operations, and other elements of the health care ecosystem nationwide.[33]

---

[28] ARMIS, *Chapter 3: A History of Medical Device Hacking*, BLOG (Nov. 9, 2022), https://www.armis.com/blog/chapter-3-a-history-of-medical-device-hacking/.
[29] *See, e.g.*, Conor Hale, *3 in 4 infusion pumps vulnerable to cyberattacks: study*, FIERCE BIOTECH (Mar. 4, 2022), https://www fiercebiotech.com/medtech/three-four-infusion-pumps-vulnerable-cyberattacks-study; Steve Alder, *Security Issues Identified in 75% of Infusion Pumps*, THE HIPAA JOURNAL (Mar. 4, 2022), https://www hipaajournal.com/security-issues-identified-in-75-of-infusion-pumps/; Medtronic*, Urgent Medical Device Correction: MiniMed™ 600 series pump system communication issue,* PRODUCT AND SERVICE UPDATES (Sept. 2022), https://www.medtronicdiabetes.com/customer-support/product-and-service-updates/notice19-letter; American Hospital Association, *H-ISAC TLP White Armis Discovers 9 Vulnerabilities in Infrastructure Used by 80% of Major Hospitals in North America*, DATA & INSIGHTS (Aug. 2, 2021), https://www.aha.org/h-isac-reports/2021-08-02-h-isac-tlp-white-armis-discovers-9-vulnerabilities-infrastructure-used-80; Nick Paul Taylor, *GE Healthcare warns of cybersecurity risks in some ultrasound software*, MEDTECH DIVE (May 15, 2024), https://www medtechdive.com/news/ge-healthcare-warns-cybersecurity-risks-ultrasound-software/716144/; CISA, *GE Healthcare Ultrasound Products (Update A),* ICS MEDICAL ADVISORY (May 16, 2024), https://www.cisa.gov/news-events/ics-medical-advisories/icsma-20-049-02.
[30] *Id.*
[31] University of California Tech News, *A sobering look at how cyberattacks on healthcare systems affect patients*, (Sept. 19, 2024), https://uctechnews.ucop.edu/cyberattacks-on-healthcare-systems-itps-presentation/.
[32] HSCC Cybersecurity Working Group, *About: What is HSCC*, https://healthsectorcouncil.org/about/health-sector-council-cyber-working-group-introduction/ (last visited Mar. 26, 2025).
[33] Raphael Satter & Christopher Bing, *US pharmacy outage triggered by 'Blackcat' ransomware at UnitedHealth unit, sources say*, REUTERS (Feb. 26, 2024), https://www.reuters.com/technology/cybersecurity/cyber-security-outage-change-healthcare-continues-sixth-straight-day-2024-02-26/.

There are also potential national security risks arising from legacy medical devices. John Riggi, national advisor for cybersecurity and risk at the American Hospital Association (AHA), has raised concerns regarding the risk associated with Chinese-made medical devices, particularly due to China's history of installing malware within U.S. critical infrastructure.[34] Moreover, when referring to the scope of the problem, Riggi explained that "we don't know because of the sheer volume of equipment in hospitals. We speculate there are, conservatively, thousands of these monitors; this is a very critical vulnerability."[35]

China's documented practice of installing malware was described in the February 7, 2024, announcement from the FBI, National Security Agency, and CISA that the Chinese state-sponsored threat actor Volt Typhoon compromised the information technology environments of multiple critical infrastructure providers in the U.S.[36] The agencies warned that Volt Typhoon had already embedded itself inside "multiple critical infrastructure organizations—primarily in communications, energy, transportation systems, and water and wastewater systems."[37] The agencies were "concerned about the potential for these actors to use their network access for disruptive effects in the event of potential geopolitical tensions and/or military conflicts."[38] In response to the government alert, the AHA issued a press release noting the guidance issued by U.S. and international authorities to help critical infrastructure sector leaders, including health care, defend their networks, and to urge health care leaders to prepare for potential disruptions, emphasizing the serious threat Volt Typhoon poses to systems that the health care sector depends on.[39]

C. FDA Law and Regulation

In December of 2022, Congress updated the laws governing cybersecurity requirements for medical devices.[40] Section 3305 of the Consolidated Appropriations Act, 2023—"Ensuring Cybersecurity of Medical Devices"—added section 524B, Ensuring Cybersecurity of Devices, to the Federal Food, Drug, and Cosmetic Act.[41] This law, also known as the PATCH Act, increased the FDA's authority over medical device cybersecurity by requiring medical device manufacturers to submit to the FDA, among other things, their plans to monitor, identify, and address cybersecurity vulnerabilities for any new medical device starting in March 2023.[42]

---

[34] Kevin Williams, *Chinese medical devices are in health systems across U.S., and the government and hospitals are worried*, CNBC CYBER REPORT (Feb. 23, 2025), https://www.cnbc.com/2025/02/23/china-made-medical-devices-are-all-over-us-and-the-feds-are-worried html.
[35] *Id.*
[36] CISA*, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, AA24-038A (Feb. 7, 2024), at 2, https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf.
[37] *Id.*
[38] *Id.*
[39] AHA, *Critical infrastructure leaders urged to secure networks from Volt Typhoon threat* (Mar. 21, 2024), https://www.aha.org/news/headline/2024-03-21-critical-infrastructure-leaders-urged-secure-networks-volt-typhoon-threat.
[40] FDA, *Cybersecurity*, DIGITAL HEALTH CENTER OF EXCELLENCE, https://www fda.gov/medical-devices/digital-health-center-excellence/cybersecurity (last visited Mar. 24, 2025).
[41] Federal Food Drug and Cosmetic Act, 21 U.S.C. §360n-2.
[42] GAO, *supra* note 8.

On September 27, 2023, the FDA's Center for Devices and Radiological Health (CDRH) issued guidance designed to minimize cybersecurity risks in medical devices.[43] The new rules prioritized a more rigorous premarket assessment of cybersecurity risk, in addition to a more comprehensive approach to post-market monitoring of cybersecurity vulnerabilities.[44] A crucial part of the effort involved ensuring that devices going to hospitals would not become quickly outdated, along with requiring manufacturers to develop specific plans for monitoring and updating or patching older software.[45]

D. Continued Challenges in Addressing Legacy Medical Device Vulnerabilities

The PATCH Act was limited to new devices and did not retroactively apply to devices made before March 2023, unless the manufacturer submits a new marketing application for changes to the device.[46] Thus, challenges remain for the older legacy devices that may be running on outdated and unsupported software. Moreover, there are reasons to believe that cybersecurity issues like the ones outlined above are present in other legacy medical devices.

For example, a March 2023 report by HSCC noted concerns with legacy medical devices present "in health care environments which cannot be reasonably protected against current cybersecurity threats."[47] The report also notes that some devices "may present risks that cannot be sufficiently mitigated to address cyber threats, as current best practices recommend."[48] Additionally, the report states that "other devices contain insufficient, poor, or no security controls, or they may have contained state-of-the-art security controls at the time they were deployed, but because of the long lifetimes" of these products, these devices now contain vulnerabilities against cybersecurity threats.[49]

Patching and software updates—while useful in many cases—often fall short in legacy devices due to outdated operating systems, hardware limitations, and lack of manufacturer support.[50] Many legacy devices were not designed to accommodate modern cybersecurity updates and cannot meet current security standards, even with interventions.[51] Full device replacement is more effective from a security standpoint but poses significant financial and operational challenges, particularly for small, rural, or under-resourced health care facilities.[52] Some hospitals may continue to use older equipment well beyond its "end of support" period, or even pass it on to other institutions, compounding the risks across the system.[53]

---

[43] FDA, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions,* CENTER FOR DEVICES AND RADIOLOGICAL HEALTH (Sept. 27, 2023), https://www.fda.gov/media/119933/download.
[44] Ricky Zipp, *4 Steps to minimize the threat of legacy medical devices*, MEDTECH DIVE (Sept. 23, 2024), https://www medtechdive.com/news/steps-minimize-threat-legacy-medical-devices/727679/.
[45] Ricky Zipp, *supra* note 13.
[46] *Id.*
[47] HSCC, *supra* note 12 at 5.
[48] *Id.*
[49] *Id.*
[50] *Id.* at 101-102.
[51] *Id*. at 5.
[52] MITRE, *supra* note 7, at 2.
[53] *Id*.

Because of the durability of the hardware in many cases, as noted *supra*, "[i]n organizations lacking the staff and resources to refresh their infrastructure, which is not uncommon, these legacy devices and their associated risks can persist indefinitely."[54] According to the HSCC's report, these legacy devices are "a proven risk" to the health care sector.[55] They have been repeatedly identified as root causes in after-action evaluations of security incidents and as continuing and stubborn challenges for both HDOs and MDMs.[56]

Despite these cybersecurity risks, legacy medical devices are still broadly used and provide important health care services.[57] Thus, simply removing these devices may present risks to patient safety and clinical operations, and replacing them altogether presents financial challenges.[58] Alternative strategies for managing these risks are necessary since cybersecurity risks are unlikely to be sufficiently mitigated through patching and updating due to outdated technology and compatibility issues.[59]

Several working groups, including the HSCC, have made "valuable" contributions toward identifying the challenges and making recommendations.[60] Still, gaps remain.[61] Challenges noted in a November 2023 MITRE Corporation report include the need for more data to inform decision-making by HDOs and MDMs as they implement risk management frameworks; clearly defining medical device lifetimes and lifecycle phases; permitting the development of shared responsibility between HDOs and MDMs, where specific roles and responsibilities may change as devices move through the lifecycle phases; and identifying resources to help some HDOs implement recommendations to address cybersecurity concerns, particularly those in less-resourced rural and safety-net facilities.[62]

IV. Previous Committee Activity

The Committee has had a sustained interest in examining legacy medical device cybersecurity issues that impact the health care sector. To highlight a few examples, the Subcommittee on Oversight and Investigations held a hearing on April 4, 2017, entitled, "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships."[63] The hearing examined the current state of public-private partnerships for cybersecurity in health care, one of 16 critical infrastructure sectors.[64] The hearing noted that the challenge lies in the fact that there is no single solution to better cybersecurity; it depends on multiple improvements, new approaches, and fresh thinking, as well as a commitment to strengthening existing institutions.[65]

---

[54] *Id*. at *5*.
[55] *Id.*
[56] *Id.*
[57] MITRE, *supra* note 7, at 1.
[58] *Id.*
[59] *Id.*
[60] *Id.* at 4.
[61] *Id.*
[62] *Id.*
[63] *Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships*, Hearing before the Subcomm. on Oversight and Investigations, H. Comm, on Energy and Commerce, 115th Congress, First Session, Serial No. 115-24 (Apr. 4, 2017), https://www.govinfo.gov/content/pkg/CHRG-115hhrg25828/pdf/CHRG-115hhrg25828.pdf.
[64] *Id.*
[65] *Id.*

In April 2018, the Committee released a Request for Information (RFI) seeking input on how to address legacy technology and related issues in the health care sector.[66] The RFI stated:

> [t]he challenges created by legacy technologies are, by definition, decades in the making. They implicate dozens of diverse stakeholders with different and at times competing equities, and they have no clear solutions. . . [t]o understand the full scope of the challenge and potential paths to address it, [the Committee requires] insight from stakeholders of all sizes, from all parts of the health care sector.[67]

In response, the Committee received nearly 300 pages worth of comments. Following the RFI's release and the receipt of comments, the Committee convened a staff-level roundtable in October 2018 with members of the health care sector to discuss how to improve transparency and clarity with regard to legacy technology risks, roles and responsibilities, and strategies.[68] In December 2018, the Committee issued a Cybersecurity Strategy Report prepared by Majority Staff, which also covered legacy medical devices.[69]

V. KEY QUESTIONS

The hearing will examine cybersecurity concerns with legacy medical devices, particularly new developments in recent months, and may include discussion around the following key questions:

- What is the current scope of the problem associated with legacy medical devices?
- How does this problem impact patients and their private health information, as well as hospitals and providers?
- What are the risks of these vulnerabilities being exploited by bad actors or nation states, such as China?
- What efforts are underway to address these vulnerabilities, and how can we better facilitate these efforts?

---

[66] *Supported Lifetimes Request for Information*, H. Comm. on Energy and Commerce, 115th Congress (Apr. 20, 2018), https://web.archive.org/web/20180924105318/https://energycommerce house.gov/wp-content/uploads/2018/04/20180420Supported_Lifetimes_RFI.pdf.
[67] *Id.* at 3.
[68] *Roundtable on Supported Lifetimes,* H. Comm. on Energy and Commerce, 115th Congress (Oct. 2018).
[69] Majority Staff of H. Comm. on Energy and Commerce, 115th Congress, *Cybersecurity Strategy Report* (Dec. 7, 2018), https://nsarchive.gwu.edu/themes/custom/nsarchive/templates/pdfjs/web/viewer.html?file=https%3A%2F%2Fnsarchive.gwu.edu%2Fsites%2Fdefault%2Ffiles%2Fdocuments%2F5686097%2FHouse-Committee-on-Energy-and-Commerce-Majority.pdf.

VI. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Majority Committee staff at (202) 225-3641.