Chairman Gary Palmer
Opening Statement—Subcommittee on Oversight and Investigations
"Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices"
April 1, 2025

As prepared for delivery

Good morning, and welcome to today's hearing entitled "Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices."

Legacy medical devices are medical devices that cannot be reasonably protected against current cybersecurity threats. In some instances, these are older devices that were made before existing cybersecurity requirements were established, but they can also be newer devices that have outdated software and lack the necessary cybersecurity protections required to defend against current threats.

There is a broad range of medical devices that can be vulnerable to cybersecurity threats, but examples include patient monitors, infusion pumps, and imaging systems. With over 6,000 hospitals in the U.S.,[1] each housing a range of rooms and beds and an average of 10 to 15 connected devices per bed,[2] it is clear how integral medical devices are to delivering health care in the U.S.

One challenge with these devices is that the hardware can last 10 to 30 years, but the software becomes obsolete much sooner. Patching and updating software are common ways to address cybersecurity vulnerabilities, but it is unlikely that such vulnerabilities can be

[1] American Hospital Association, Fast Facts on U.S. Hospitals, 2025 (updated Jan. 2025). https://www.aha.org/statistics/fast-facts-us-hospitals

[2] Steve Alder, 63% of known exploited vulnerabilities can be found in hospital networks, THE HIPAA JOURNAL (Mar. 12, 2024), https://www hipaajournal.com/security-issues-identified-in-75-of-infusion-pumps/

sufficiently mitigated through these approaches due to outdated technology and compatibility issues.

Moreover, merely replacing devices comes with financial and logistical challenges which leads many hospitals to retain these legacy medical devices well beyond their life expectancies – often without the software support to handle modern cybersecurity risks. This is particularly true in small, rural, or under-resourced facilities, making it crucial to find practical solutions.

It is also important to recognize that the health care sector is one of 16 critical infrastructure sectors in the U.S., and it has become a significant target for cyberattacks. For example, in 2017, the global WannaCry ransomware attack severely impacted the health care sector. In the U.S., medical device manufacturers rushed to patch affected devices after WannaCry showed that malware could jump from PCs to embedded medical devices. This attack demonstrated how unpatched, older Windows-based systems in medical devices can be immobilized by ransomware.

Additionally, the risk of harm to patients is a big concern because if a medical device's vulnerability is exploited, the ability for a device to help monitor, diagnose, or treat a patient can be compromised.

There are also national security concerns. On January 30th, the Cybersecurity and Infrastructure Security Agency and the Food and Drug Administration (FDA) released an alert about a Chinese-made patient monitor that had a hidden backdoor that could enable remote control and data exfiltration. While the vulnerability may have been unintentional, it raised concerns and highlighted the risk of nation-state actors pre-positioning destructive malware in

our health care sector as part of a potential, large-scale cyberattack to disrupt one of our nation's critical infrastructure sectors.

Progress was made to address legacy medical device issues in 2022, with the enactment of the PATCH Act which increased FDA's authority over medical device cybersecurity. The law now requires manufacturers to submit cybersecurity plans for new devices. Legacy medical devices that were on the market before this law took effect, however, still pose a significant risk.

Therefore, addressing cybersecurity threats in legacy medical devices is critical. Fortunately, thanks to the ongoing work of the experts represented by our witnesses today, we have valuable partnerships and coordinated efforts to help address these risks and threats.

I thank our witnesses for joining us today and sharing their expertise to guide the efforts in addressing these challenges, and I look forward to their testimony.

I now recognize the Ranking Member of the Subcommittee, Ms. Clarke, for her opening statement.