Chairman Brett Guthrie
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

Chairman Palmer, thank you for holding this important oversight hearing on cybersecurity vulnerabilities in legacy medical devices. The vulnerabilities in these devices pose serious risks to patient safety, care delivery, and the resilience of our health care infrastructure which makes it critical to our health care ecosystem and national security that we examine this issue.

Legacy medical devices are devices that cannot be reasonably protected against current cybersecurity threats, regardless of when they were manufactured. These include technologies such as patient monitors, infusion pumps, implantable devices, and diagnostic equipment that hospitals and patients rely on every day.

According to a cybersecurity firm report cited by the FBI, as of January 2022, "53% of connected medical devices and other internet of things (IoT) devices in hospitals had known critical vulnerabilities."[1] This figure illustrates the potential scope of the problem.

In 2022, Congress passed the PATCH Act, which enhanced the FDA's authority over cybersecurity for new medical devices. This was an important step forward, but it only applies to new devices, leaving older devices unaddressed.[2] This leaves a significant gap in our defenses.

[1] https://www.ic3.gov/CSA/2022/220912.pdf
[2] https://www.medtechdive.com/news/medical-device-cybersecurity-risks-future/712112

In January, the federal government issued an alert about the discovery of a patient monitor made in China that had been in the U.S. market since 2011.[3] The device, made by Contec [CON-TECH] Medical Systems in China, was configured to connect to an IP address belonging to a University in Beijing, which had no apparent connection with the manufacturer.

According to the Cybersecurity and Infrastructure Security Agency, the backdoor enables the IP address at the university to remotely download and execute unverified files on the patient monitor. Moreover, a cybersecurity firm noted that hackers working from the university to which the patient monitor's backdoor is connected targeted U.S. energy companies, communications companies, and the state government of Alaska in 2018.[4] Regardless of whether the patient monitor is just a low-quality product with inadequate cybersecurity controls, *or* its design was intentional, the discovery is concerning from a patient safety and national security perspective.

FDA issued a safety communication with recommendations for health care providers and patients on how to mitigate the risk with this device. While we, thankfully, have no indication of direct harm caused by the vulnerability in these patient monitors the risks identified call attention to the patient safety risks posed by vulnerabilities in legacy medical devices. Another example that is illustrative of these risks is that "there 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."[5]

---

[3] https://www.cisa.gov/resources-tools/resources/contec-cms8000-contains-backdoor; https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-patient-monitors-contec-and-epsimed-fda-safety-communication.

[4] https://www.reuters.com/article/world/chinese-hackers-targeted-us-firms-government-after-trade-mission-researchers-idUSKBN1L11DX/.

[5] https://uctechnews.ucop.edu/cyberattacks-on-healthcare-systems-itps-presentation/.

Additionally, compromised devices can serve as entry points for larger network attacks, potentially disrupting hospital operations or exposing sensitive patient data.

Stakeholders, including medical device manufacturers, health care delivery organizations, cybersecurity experts, and the federal government have been coordinating to address these risks, but challenges remain. We must continue to support these efforts to ensure comprehensive protection of our health care infrastructure.

I thank Chairman Palmer for holding this hearing. This discussion will help us continue to address pressing technological concerns, protect patients, and help us close national security gaps.

Thank you, and I look forward to hearing from our witnesses today.