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

April 23, 2025

Mr. Erik Decker
Vice President and Chief Information Security Officer
Intermountain Healthcare
4646 Lake Park Boulevard
Salt Lake City, UT 84120

Dear Mr. Decker:

Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, April 1, 2025, to testify at the hearing entitled "Aging Technology, Emerging Threats: Examining Cybersecurity Vulnerabilities in Legacy Medical Devices."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Wednesday, May 7, 2025. Your responses should be mailed to Emma Schultheis, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to Emma.Schultheis@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Gary Palmer
Chairman
Subcommittee on Oversight and Investigations

cc: Yvette Clarke, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

Attachment — Additional Questions for the Record

The Honorable Russ Fulcher

1. Mr. Decker, I would like to narrow down on different cybersecurity threats that could impact clinics like Intermountain Health, as well as hospitals and other healthcare delivery organizations. In your testimony, you raised concerns about foreign governments like China, Russia, and others "infiltrating" software or hacking into network hardware like routers or switches. How big of a problem is it for clinics to ensure there is not malware that might change the readings of a patient, causing a change in stimulus on a cardiac pacemaker or defibrillator, or a change in the dosage amounts on an insulin pump due to misrepresented readings?

2. Could you expand on your recommendation to be able to share classified information on potential threats throughout the healthcare industry?

    a. It also sounds like threat information you receive from agencies like the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are not easily accessible or easily digestible?

    b. Any improvements to simplify or consolidate?

The Honorable Russ Fulcher:

Mr. Decker, I would like to narrow down on different cybersecurity threats that could impact clinics like Intermountain Health, as well as hospitals and other healthcare delivery organizations. In your testimony, you raised concerns about foreign governments like China, Russia, and others "infiltrating" software or hacking into network hardware like routers or switches. How big of a problem is it for clinics to ensure there is not malware that might change the readings of a patient, causing a change in stimulus on a cardiac pacemaker or defibrillator, or a change in the dosage amounts on an insulin pump due to misrepresented readings?

Honorable Rep. Fulcher, thank you for the astute question about a concerning topic. The question boils down to the impact that hacking, or malware, could cause to patients through either direct impact (such as pacemakers or defibrillators) or through indirect impact (through changing readings and the integrity of data resident within the devices that are used for clinical decision making).

The answer to this question directly relates to the motivation and nature of bad actors that would have an interest in conducting such attacks. In two of the referenced attacks, localized access would likely be necessary. This is because pacemakers, defibrillators and insulin pumps require local access to maintain, adjust, or set dosages. While this does lower the attack surface of the attack, making it less likely at wide scale, it doesn't entirely prevent such attacks. Probably the most likely attack of this nature would be a highly targeted attack on a specific person of interest by, for example, a motivated and well-resourced actor, such as a nation state. In fact, in 2007, former Vice President Dick Cheney ended up replacing his pacemaker with a device that was not wireless capable.

It is important to note that there have been no publicly reported cyber attacks on implanted or connected medical devices that have caused harm to specific patients.

Regarding an attack against the integrity of readings of patients, the concerns are more nuanced. Medical device manufacturers have raised concerns about so-called AI Poisoning Attacks, by which the data used to train models has been maliciously adjusted to cause unreliable outputs. Additionally, there has been some science that has shown how - due to the unencrypted nature of the internal medical transaction system- it *could* be possible to manipulate radiological images of patients to add or remove cancer nodules, thus fooling radiologists that read the studies. This was a proof of concept research study conducted by the Ben-Gurion University of Negev, titled "CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning". These studies and attacks are concerning, but there are no known publicly reported cases of them happening.

I think it's important to keep an eye on the horizon, thinking ahead about where the adversary could shift to. Attacks against the integrity of medical data is very much a fear amongst the cybersecurity community. However, we are also dealing with the very real, and very damaging threat today, of Organized Crime conducting ransomware attacks against hospital systems across the country. This threat is here, right now.

In fact, one study conducted by Hannah Neprash, Claire McGlave, and Sayeh Nikpay from the University of Minnesota showed that among patients already admitted to a hospital when a ransomware attack begins, in-hospital mortality increases by 35-41%. This study was titled "Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients". It demonstrates there is very real harm happening right now, harm that is not theoretical.

It is critical that we defend accordingly. This must be done in a joint and collaborative manner between Critical Infrastructure, the Administration, and Congress. As I stated in my written testimony, I believe the following actions should be taken to combat all of these threats:

1. Reinstate, and codify, the Critical Infrastructure Policy Advisory Committee, which allows Critical Infrastructure and the Federal Government to partner in a protected forum and collaborative manner
2. Kick off a Cleared Task Force, amongst members of Critical Infrastructure that hold clearances (or are sponsored to achieve clearance), and our national intelligence security apparatus. This Task Force should look at the very sensitive intelligence to help answer these theoretical but vital questions, and provide a series of recommendations to defend accordingly.
3. Amplify and continue to encourage participation in Sector Coordinating Councils, like the Health and Public Health Sector Coordinating Council Cybersecurity Working Group. This is the forum to tackle these complicated questions.

The Honorable Russ Fulcher:
Could you expand on your recommendation to be able to share classified information on potential threats throughout the healthcare industry?

a. **It also sounds like threat information you receive from agencies like the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are not easily accessible or easily digestible?**

   CISA and the FBI do produce flash reports on a regular basis warning Critical Infrastructure of specific vulnerabilities and/or potential threat actors. These reports are good, though it requires a level of sophistication and knowledge as well as sufficient time to a) know about the existence of the reports and b) act accordingly and with the urgency required.

   We can always improve, and should continue to push for improvement. One of the challenges is how to determine the criticality, priority, and action related to these flash reports. They don't come with the same level of urgency as, say, a Tornado Warning system that a population understands. Additionally, when there have been highly disruptive attacks, such as WannaCry, Not Petya, or Change Healthcare, the response of the national apparatus and Critical Infrastructure continues to be sowed with confusion, misinformation, and delays. During the moments of highest need we cannot get the relevant information we need to protect our organizations.

   Case in point, during Change Healthcare, the initial intrusion vector was not concretely known until Andrew Witty testified to Congress that it was a lack of Multifactor Authentication on a Citrix server. During the early stages of the attack CISOs across the country were told that the attack happened through a remote access tool. Hundreds and thousands of hours were spent chasing that rumor. Organizations started discovering, patching, and replacing this technology thinking that they could be next. We are now blessed with hindsight to know that was not the attack vector, and perhaps some of those emergency patches actually helped protect against other attacks, however it was misdirected due to the lack of this real information sharing.

   We need the ability to know the real vectors of attack within 24 hours of the attacks occurring in order to stay ahead of our adversary. This requires more than flash reports from CISA and the FBI about critical vulnerabilities. It requires active collaboration, coordination, facilitation and logistics.

Intermountain Health

b. Any improvements to simplify or consolidate

A few suggestions:

1. Reduce legal burden and ensure the protection of information sharing of explicit attack vectors. This was done under the Cybersecurity Act of 2015, however many organizations do not know this and fear a civil action taken against them by 'admitting' being hacked through the sharing of the details of the hack.

2. Ensure that once CISA receives ransomware notifications under CIRCIA that it is redistributed back to the Critical Infrastructure sectors within 24 hours through automated systems

3. Put real stimulus into the hands of needs-based hospitals through ongoing reimbursements, directly funding the establishment of cyber programs and incident response teams. Our most vulnerable hospitals do not have the cyber sophistication to be reactive, in real time, to the nature of adversary. In many cases, these hospitals are the sole provider of acute care within a 60 miles radius in rural areas.

4. As former National Cyber Director Chris Inglis said:

   The job needs to be approached not as a simple division of labor, but as a move towards collective defense.

   "We have to use all of our capabilities, all of our parties, all of our sightlines to figure out when one of us catches something – some nuance, some loose thread – compare that immediately with the other insights, hunches, threads, shards of information that someone else may have," he said. "So that together, we can discover something no one of us can discover alone and, frankly, get to a place where if you're an adversary in this space, you got to beat all of us to beat one of us."